

IN THE UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF MASSACHUSETTS

ALLIANCE FOR AUTOMOTIVE  
INNOVATION

Plaintiff,

vs.

MAURA HEALEY, ATTORNEY GENERAL  
OF THE COMMONWEALTH OF  
MASSACHUSETTS in her official capacity,

Defendant.

C.A. No. 1:20-cv-12090-DPW

**Leave to File Under Seal  
Granted July 13, 2021**

**PLAINTIFF'S POST-TRIAL PROPOSED FINDINGS OF FACT  
AND CONCLUSIONS OF LAW\***

**FINDINGS OF FACT**

**Introduction**

1. Plaintiff Alliance for Automotive Innovation (“Auto Innovators” or “Plaintiff”) is a trade association comprising auto manufacturers that, together, produce almost 99 percent of vehicles sold in the United States today. Douglas Aff. ¶ 2.

2. In 2020, FCA US LLC (“FCA”), now under the parent company Stellantis N.V., shipped more than 3.4 million vehicles for sale worldwide. FCA sells approximately 35,000 – 40,000 vehicles annually in Massachusetts. Chernoby Aff. ¶ 2. As of November 29, 2020, there were approximately 16,070 FCA vehicles currently on Massachusetts dealership lots, consisting primarily of about 14,300 Model Year 2021 vehicles that have already undergone rigorous design and testing. *Id.* ¶ 3.

\* Certain passages of the publicly-filed version of this document have been redacted to reflect those portions of the trial evidence that the plaintiff still contends should be sealed as “confidential” or “highly confidential.” See ECF #228. The Attorney General redacts these passages without conceding that they, or any portion of the trial evidence, are entitled to be sealed, and without prejudice to her right to oppose any sealing proposed by the plaintiff.

Marked Response filed by Defendant AG Healey:  
/s/ Eric A. Haskell July 20, 2021  
Robert E. Toone, BBO No. 663249  
Eric A. Haskell, BBO No. 665533  
Phoebe Fischer-Groban, BBO No. 687068  
Assistant Attorneys General  
Christine Fimognari, BBO No. 703410  
Special Assistant Attorney General  
One Ashburton Place, Boston, Mass. 02108  
(617) 963-2855 / eric.haskell@mass.gov

3. In 2020, General Motors (“GM”) shipped approximately 7 million vehicles worldwide, including about 2.5 million sold in the United States alone. Tierney Aff. ¶ 3. As with FCA, many GM vehicles are sold in the Commonwealth of Massachusetts every year; in 2020, GM delivered almost 30,000 vehicles to Massachusetts. *Id.*

4. [FCA and GM are representative of Auto Innovators’ membership more generally. Most vehicle architecture approaches and cybersecurity best practices are the same or similar across manufacturers.] June 14 Tr. 199:19-24 (Bort). All of Auto Innovators’ members—not just FCA and GM—employ cybersecurity systems to protect their vehicles and restrict access to vehicle systems to ensure that their systems remain functional. *See, e.g.*, Smith Aff. ¶¶ 141, 154 (noting that OEMs generally use various cybersecurity techniques to secure vehicle functions); Bort Aff. ¶ 54 (“OEMs employ various authorization mechanisms before providing access” to diagnostic data and functions); Garrie Aff. ¶ 8 (“Modern automobiles have built-in cybersecurity features that are part of the automobile’s design and protect safety-critical and emissions-related components”); June 15 Tr. 197:10-14 (Romansky not aware of manufacturers who have removed themselves from authorization process for access to vehicle on-board diagnostic systems).

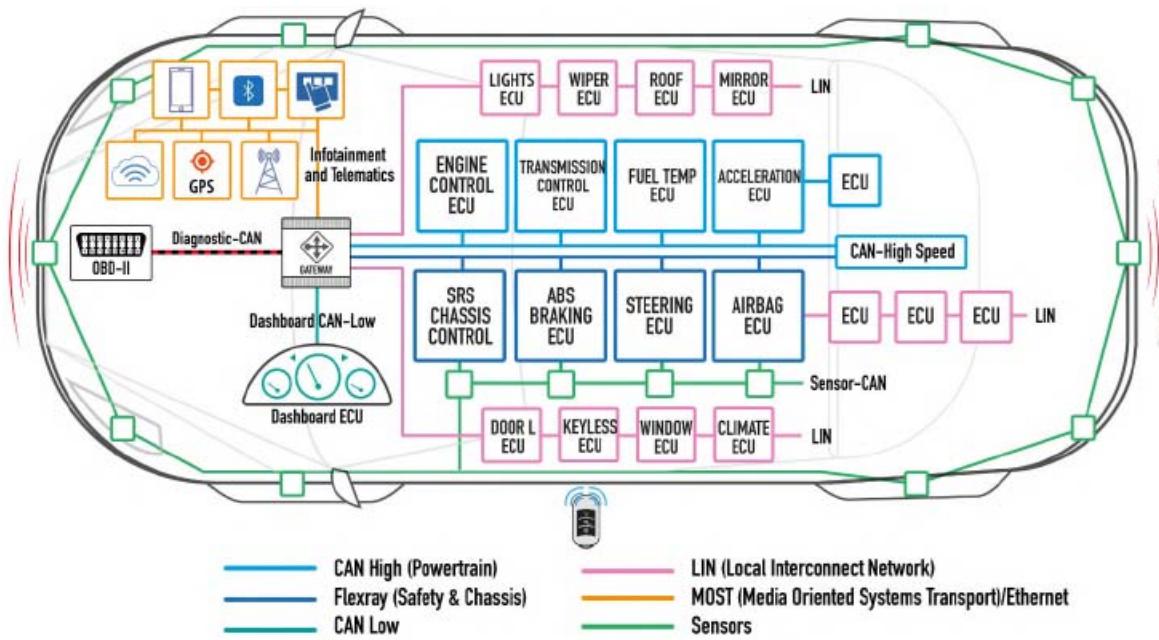
5. [Likewise, motor vehicle manufacturers as a whole are similarly situated in their inability to comply simultaneously with federal law and the various requirements in Massachusetts Ballot Question No. 1, titled *An Act to Enhance, Update and Protect the 2013 Motor Vehicle Right to Repair Law*, now codified at Chapter 93K of the Massachusetts General Laws (“the Data Access Law”)]. As of the fall of 2020, December 3, 2020, and the time of trial, no OEMs can comply with the Data Access Law. June 16 Tr. 41:11-42:10 (all of the parties’ experts agreeing that no OEMs could meet the requirements of the Data Access Law as of those times). To attempt to comply with the Data Access Law, Auto Innovators’ members would have to alter their vehicles in a

manner that would increase the cybersecurity risks to safety- and emissions-critical vehicle systems.] See, e.g., June 14 Tr. 200:20-201:8 (Bort) (“[I]nherently, compliance requires the abrogation of the protections that have been built into them that have just been layered and built up over time.”); June 14 Tr. 70:6-21, 71:18-72:3, 73:14-22 (Tierney) (explaining how compliance with the Data Access law would require removal of critical GM functions); June 15 Tr. 113:3-21 (Smith) (confirming that “the Data Access Law would require OEMs to make changes to the cybersecurity they have on their vehicles today”; that “altering cyber protections that exist on a vehicle could make them more vulnerable to cyber attacks”; that “with the correct access, hackers can take over core functionality of a vehicle”; and that hackers could “thwart safety systems or install malware on a vehicle,” among other possibilities); Garrie Aff. ¶ 64 (“To comply with the Data [Access] Law, OEMs would have to remove or alter critical cybersecurity controls, which would substantially increase the safety risks of using their vehicles”); [see also U.S. Statement of Interest (Dkt. 202) at 8 (“the Data Law requires motor vehicle manufacturers to take actions that potentially pose serious cybersecurity risks by opening uncontrolled access to vehicle firmware that executes safety-critical functions, such as steering, acceleration, and braking, which are designed in a manner that expect (and require) authenticated privileged access rights in existing implementations”).]

## Vehicle Cybersecurity

### A. Vehicle Electrical Architecture<sup>†</sup>

6. Today's vehicles are complex computing machines, with computers controlling almost every aspect of vehicle functionality. Chernobyl Aff. ¶ 35; Tierney Aff. ¶ 30; Garrie Aff. ¶ 7. The main computer components used in vehicles are electronic control units ("ECUs"), safety sensors, the Controller Area Network ("CAN"), on-board diagnostics ("OBD"), telematics systems, and the gateway. Tierney Aff. ¶¶ 31-36; Chernobyl Aff. ¶¶ 35-36; Garrie Aff. ¶ 20; Smith Aff. ¶¶ 27-28, 37, 48-51, 58. These are shown in the following diagram:



<sup>†</sup> As to the plaintiff's proposed findings ¶¶ 6-61:

- Insofar as they purport to describe actions, inactions, viewpoints, or products of an OEM(s) *other than GM and FCA*, the Attorney General both disputes the admissibility of those proposed findings and does not concede their truth. Such proposed findings are not underlined or bracketed in ¶¶ 6-61, in the interest of helping the Court to identify those proposed findings that are disputed insofar as they pertain to GM and FCA.
- Insofar as they purport to describe actions, inactions, viewpoints, or products of *GM or FCA*, the Attorney General has used [bracketing] to identify proposed findings whose admissibility is disputed, and underlining to identify proposed findings whose truth is disputed.

*ECUs and Safety Sensors*

7. As shown in the diagram, ECUs govern individual vehicle features ranging from vital functions such as engine control, acceleration, steering, anti-lock braking systems (“ABS”), and airbags to customer conveniences like climate control and keyless entry. Tierney Aff. ¶¶ 31-32. Each ECU has a specialized function. Garrie Aff. ¶ 21; Smith Aff. ¶ 28.

8. Safety sensors feed information to ECUs for the ECUs to provide the correct vehicle functionality. Tierney Aff. ¶ 33. These sensors capture and transmit information about the external environment. *Id.* Sensors gather information and then send it to the ECUs. *Id.* For example, the information that sensors gather could be about how close a vehicle is to a collision, which might then trigger seatbelt tension, or information about a vehicle’s speed, which might then trigger the correct amount of fuel injection to the engine. *Id.*; Garrie Aff. ¶¶ 27-28.

9. These computing components are connected to each other and communicate primarily through the CAN. Tierney Aff. ¶ 34; Garrie Aff. ¶ 25. The CAN is the wiring that connects the ECUs, sensors, gateway, and other vehicle components. *Id.*

*Controller Area Network*

10. The CAN transmits messages between the various components. Garrie Aff. ¶ 25; Smith Aff. ¶¶ 37-40. For example, if a driver were to start a vehicle remotely, the vehicle’s CAN would transmit a message from the telematics system that received the message to the gateway and then—after the gateway had performed such measures as challenge and response protocols and message authentication via secured keys to help to ensure that the message is valid and safe, as discussed below—to the ECUs that control the engine. Garrie Aff. ¶ 25.

*On-Board Diagnostic Systems*

11. OBD software monitors vehicles for maintenance issues. Chernoby Aff. ¶ 36.

Since at least 1996, federal law has required second-generation OBD, called OBD-II, to monitor emissions systems. *Id.*; *see also* Smith Aff. ¶¶ 48, 50. While federal law requires OBD-II only for emissions purposes, most auto manufacturers have designed their OBD-II systems to diagnose a much larger set of potential issues. Tierney Aff. ¶ 39; Chernoby Aff. ¶ 37; Garrie Aff. ¶ 31.

12. Technicians (including both franchised dealers and independent repair shops) can connect to the vehicle through an OBD-II port and receive codes about what part of the vehicle needs maintenance or repairs. Chernoby Aff. ¶ 37; Ex. 9 (AAI-FCA-11200); Garrie Aff. ¶ 31. Technicians connect to this port with a physical tool (often called a “scan tool”). Smith Aff. ¶¶ 52-53. The scan tool has the ability to run certain diagnostics on the vehicle based on the information the OEM provides to the scan tool manufacturer. *Id.* ¶¶ 52-53, 147.

13. Different diagnostics require different security authorization levels. *Id.* ¶ 146. For example, diagnostics that query a vehicle for limited data do not require authorization, and thus are available via “anonymous access.” *Id.* However, additional authorization is required for more involved diagnosis, as well as repair and maintenance functionality. *Id.*

14. In order fully to access a vehicle’s OBD system to repair vehicles, technicians may also send diagnostic commands, referred to as “writing,” that cause the vehicle to execute a certain function, such as moving the dials on the dashboard, or modify the software on the ECUs. Smith Aff. ¶ 53; Chernoby Aff. ¶ 38; Tierney Aff. ¶ 39; Garrie Aff. ¶ 31. The ability to write to vehicles in addition to reading diagnostic codes is integral to repair. June 15 Tr. 82:23-83:12 (Lowe) (testifying that “write commands and bi-directional capabilities” are “critical” to repairs and explaining that technicians frequently have to download the latest software updates to a vehicle to

complete the repair); Smith Aff. ¶ 142 (“To fully support all mechanical diagnostics and repairs, independent repair shops and vehicle owners need to be able to perform three types of actions: (1) communicate through the gateway, (2) read and write diagnostic data to each ECU, and (3) transmit packets to the ECUs.”).

15. The OBD diagnostic codes that tell a technician what to repair for emissions purposes are standard across the industry. *See* Smith Aff. ¶ 50 (“Federal regulations require emissions-related data to be made available through the OBD-II port.”). But additional diagnostic functions available within a given OBD system and the software used to make updates to vehicle ECUs are non-standardized and specific to each manufacturer. *See* June 14 Tr. 214:3-9 (Bort) (“there are elements beyond what the core OBD-II port has that are there, they’re not standardized”); Smith Aff. ¶¶ 125-26, 147 (“Not all DTCs [Diagnostic Trouble Codes] are currently shared as part of the UDS [Unified Diagnostic Services] standard,” and there is a “gap in standardization” for “diagnostics information and repair methodologies”). For instance, the pins that comprise the OBD port and provide access are not all standardized, which results in variation in information available via the port. *See, e.g.*, Smith Aff. ¶¶ 49, 51 (“pins can vary for each make, model, and year of vehicle” and “each OEM decides which information is available through the unregulated pins on the OBD-II port”). These non-standardized elements that OEMs provide to repair technicians are necessary to conduct repairs. *See, e.g.*, June 15 Tr. 109:18-24 (Potter) (“To repair that vehicle, you need to have further information than what you do in your standardized reporting”).

16. There are good reasons why variation exists among OEMs’ OBD systems. Standardized software would expand potential cybersecurity threats (by giving a hacker one common point of entry to all manufacturers’ systems) and hinder the traceability of any breaches.

Bort Aff. ¶ 65; Chernoboy Aff. ¶ 72; Tierney Aff. ¶ 92. And manufacturers are necessarily involved in the process of writing updates to vehicle systems because they alone are uniquely positioned to develop, test, and certify that software, securely release it, and then maintain its security. Tierney Aff. ¶¶ 108-10. Someone has to play the role of gatekeeper and adding another entity between the manufacturer and the end-user by definition increases the risk potential. Tierney Aff. ¶ 94. This is even more true if manufacturers are cut out of the process entirely by being deprived of any direct or indirect control over some new middleman gatekeeper. *Id.*

*Telematics Systems*

17. Most vehicles also have a telematics system that allows a vehicle to communicate remotely, enabling features such as GPS, emergency response, and remote start. Garrie Aff. ¶ 34. For instance, GM has long used its “OnStar” system for these purposes. Tierney Aff. ¶ 36. The telematics control unit connects to the CAN, which is separated by a gateway from the “clean” side of ECUs that control the vehicle’s safety- and emissions-critical functions. *See* Ex. 41 (AAI-GM-0001567) (discussed below).

18. Telematics systems can also allow manufacturers to communicate recall information to consumers and deliver firmware over-the-air (“FOTA”) updates, [which allow for quicker and more comprehensive patching than traditional in-the-shop vehicle recalls.] Tierney Aff. ¶ 36; Chernoboy Aff. ¶ 41.

19. Telematics systems do not, however, provide manufacturer-affiliated dealerships or independent repair shops with vehicle diagnostic, repair, and maintenance data. Chernoboy Aff. ¶ 43; Tierney Aff. ¶ 37. The type of data used to conduct traditional vehicle repairs flows instead through vehicle OBD ports. *Id.*

*Gateway*

20. The “gateway” manages communications in the vehicle, allowing different ECUs to communicate with each other. Tierney Aff. ¶ 63; Garrie Aff. ¶¶ 35-37. The gateway also serves as an important firewall between the vehicle’s electrical architecture and any unauthorized access. Chernoby Aff. ¶ 49; Garrie Aff. ¶ 39.

*Development Timeline*

21. Because of the complex structure, as well as corresponding cybersecurity controls that must be put in place and testing for compliance with regulations, it takes several years of lead time to institute design changes before a vehicle is brought to market. See, e.g., June 14 Tr. 200:20-201:8 (Bort) (“the supply chain in this industry cannot just turn on a dime, and it takes a number of years to implement these changes.”); Ex. 62 at AAI-ACA-0038565 (“Historically, automakers lock in the design of a production model three to five years before its market introduction”); Smith Aff. ¶ 35 (“Design and procurement of a new ECU, including appropriate testing, may take several years, in part because suppliers of ECUs require lead time to make significant changes to their products.”). For instance, GM completed its process for model year 2022 vehicles in 2020 and is currently finalizing its model year 2023 vehicles. See Tierney Aff. ¶ 7. There is substantial lead time for vehicles’ electronic architecture in particular. For example, GM finalized the electrical components in its model year 2022 vehicles—which launch at various times throughout calendar year 2021—years earlier, between April 2017 and no later than June 2019 depending on the model. Tierney Aff. ¶ 8. FCA similarly locks down hardware designs about two years before production. Chernoby Aff. ¶¶ 5-6.

22. Manufacturers start selling vehicles in the calendar year preceding the model year. For example, manufacturers will start to sell model year 2022 vehicles during 2021. June 15 Tr. 93:7-9 (Potter).

**B. Vehicle Cybersecurity Protections**

23. The increased reliance on computers to control vital vehicle functions brings with it the threat of cybersecurity attack, whether from hostile nation-states or from hackers seeking to extract money or cause disruption. Garrie Aff. ¶ 12; Bort Aff. ¶ 19.

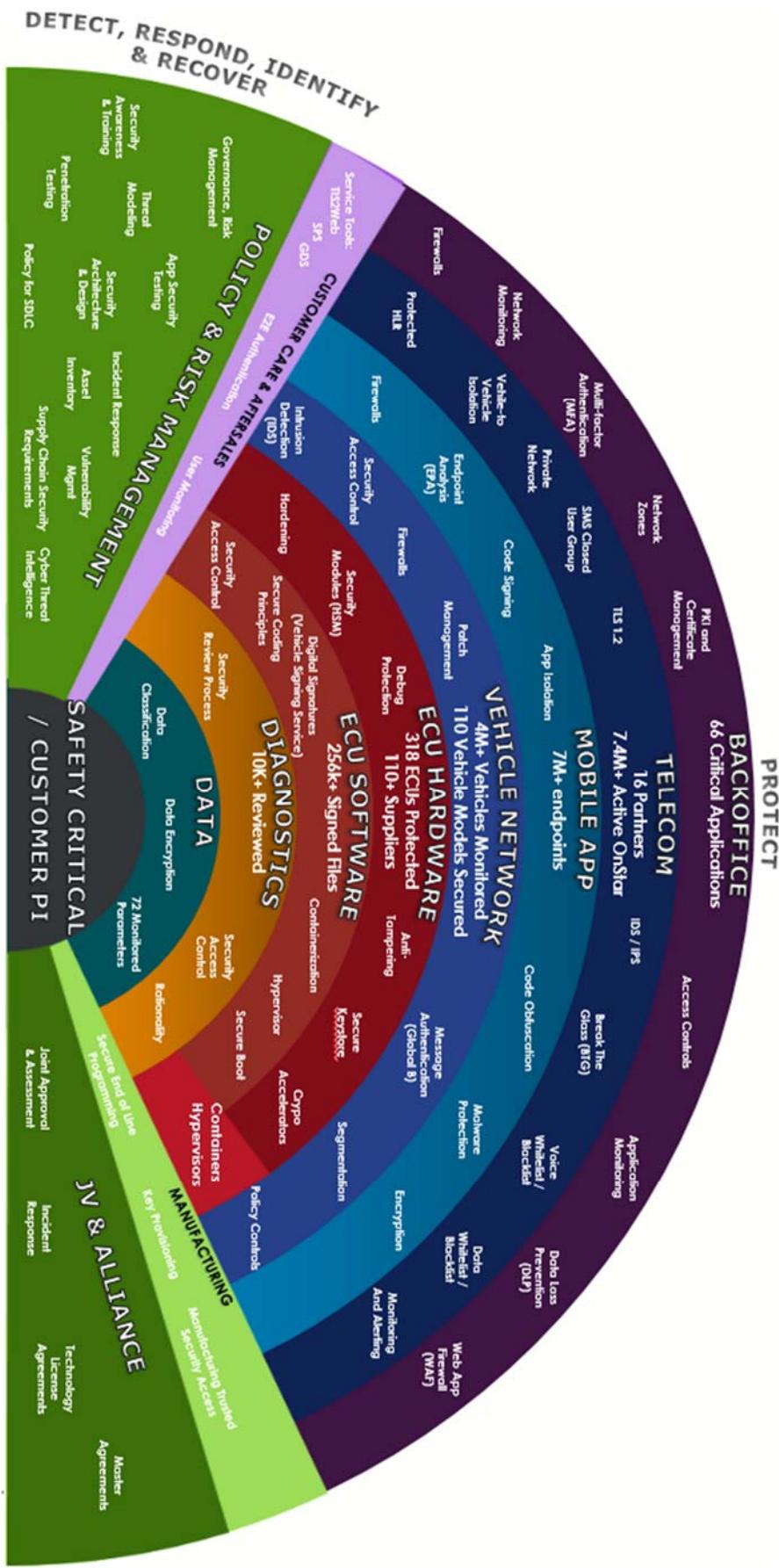
24. To protect core safety functions and emissions controls, vehicle manufacturers have developed and implemented various cyber protections around core safety functions and emissions controls. Chernoby Aff. ¶ 26; Tierney Aff. ¶ 42. [These cyber protections are elements of the design of these safety and emissions functions.] Tierney Aff. ¶ 82; Chernoby Aff. ¶ 61.

25. Current vehicles employ several layers of interdependent cybersecurity protections. Bort Aff. ¶ 27; Tierney Aff. ¶ 40-41; Chernoby Aff. ¶ 45. These layers ensure that if one layer of security is breached, other security measures can act to prevent a threat actor from compromising a vehicle. Bort Aff. ¶¶ 29-31. And manufacturers continually update their cybersecurity features to address new challenges. Tierney Aff. ¶ 20; Chernoby Aff. ¶ 27.

26. The cybersecurity guidance issued by the National Highway Traffic Safety Administration (“NHTSA”) calls for the use of a “layered approach” to vehicle cybersecurity, specifically recommending many of the controls that manufacturers currently use. Ex. 3 (NHTSA, *Cybersecurity Best Practices for the Safety of Modern Vehicles* (2016), [www.nhtsa.gov/sites/nhtsa.gov/files/documents/812333\\_cybersecurityformodernvehicles.pdf](http://www.nhtsa.gov/sites/nhtsa.gov/files/documents/812333_cybersecurityformodernvehicles.pdf)) (“NHTSA Cybersecurity Best Practices”). To take just a few examples, NHTSA Cybersecurity Best Practices calls for the use of some form of encryption to control access to firmware, *id.* at

6.7.4; directs that OEMs “[l]imit[] the ability to modify firmware,” *id.* at 6.7.5; and directs that they employ logical and physical isolation, including by isolating safety ECUs from network-connected features, *id.* at 6.7.7, 6.7.8. As shown and described below, GM and FCA have implemented their cyber protections as design elements in a layered approach, exactly as NHTSA has specified.

27. For example, GM secures the cyber safety of its vehicles with numerous separate protections, including: (1) encryption keys; (2) unique identifiers for each vehicle component, so that when one component transmits a message, the receiving component knows from which component the message came; (3) password protections; (4) secure communication channels between onboard vehicle systems and offboard computer servers; (5) in-vehicle network message authentication; (6) intrusion detection and prevention systems; (6) software authenticity and integrity checks, which safeguard vehicle component firmware programming and bootloader execution; (7) challenge and response protocols; (8) rationality checks, which control the availability and execution of safety and security-critical diagnostic routines; (9) secure storage controls, which safeguard sensitive personal and vehicle information; (10) network domain segregation; (11) logical and physical isolation; and (12) firewalls designed to control and protect the flow of messages among vehicle systems. Tierney Aff. ¶ 42. These various, layered protections are illustrated well in Exhibit 16 (AAI-GM-0000035) (on the next page):



28. Similarly, FCA secures the cyber safety of its vehicles with numerous protections, including its secure gateway, message authentication, embedded authentication to vehicle software, secure radio, and a firewall around connected features. See Chernobyl Aff. ¶¶ 45-55.

*Challenge-and-Response Protocols*

29. Challenge-and-response protocols are a security control that OEMs like GM and FCA use to protect safety-critical systems and emissions controls. *See, e.g.*, Tierney Aff. ¶ 43; Chernobyl Aff. ¶ 54.

30. In a challenge-and-response protocol, when a diagnostic tool requests access to protected vehicle data or functions, a “challenge” is issued. June 14 Tr. 113:5-22 (Baltes); Tierney Aff. ¶ 44; Chernobyl Aff. ¶ 53; Garrie Aff. ¶ 56; Smith ¶ 184. The tool then has to give the correct “response” before the component will “unlock” the requested data or function. *Id.* To give the correct response, the tool either must be programmed with a response from the OEM (*see* Potter Aff. ¶¶ 47-48) or communicate with the OEM’s back office which sends the answer to the tool. *See* Baltes Aff. ¶ 16; June 14 Tr. 99:17-100:12 (Baltes).

31. Those protocols ensure that only authorized users and devices are accessing ECUs for diagnosis, maintenance, and repair. *See, e.g.*, Garrie Aff. ¶ 57 (“Challenge/response protocols are commonly used to secure diagnostic protocols in vehicles to ensure that only authorized devices and users are accessing diagnostic components.”); Smith Aff. ¶¶ 143-44, 184 (ECUs in vehicles “validate diagnostic and repair access,” including through challenge-response protocols like Mode 27, by “check[ing] the authorized level of access before allowing write access”); *id.* Smith Aff. ¶ 146 (explaining that OEMs define different security levels for accessing their vehicles’ diagnostic functions); June 14 Tr. 113:5-12 (Baltes) (“The vehicle has a lot of diagnostics, and not all diagnostics are meant for all users. And so with our secure unlock we can

restrict diagnostics to particular user bases so it doesn't allow unrestricted access to everyone to perform all diagnostics, and it's all within the intent of keeping the motorist and repair person safe."); Baltes Aff. ¶ 16 (explaining that secure unlock is a form of challenge-response protocol).

32. Thus, challenge-and-response protocols are a form of authorization that a manufacturer imposes on access to vehicles' on-board diagnostic systems. *See, e.g.*, Smith Aff. ¶ 144 ("Since each ECU checks the level of access before allowing write access, attackers are prevented from accessing these diagnostic functions without the requisite authorization"); *id.* ¶ 146 (diagnostics "that do not require authorization" are at the security level of "anonymous access," but that OEMs impose authorization requirements on other access to diagnostic functionality); Romansky Aff. ¶ 20 ("[A]uthentication and authorization are terms used to describe the process of validating the identity and authentic access rights of a remote user or system. For example, when a repair technician uses a scan tool to read or write to an ECU within a vehicle, the vehicle network can optionally require that the technician or the scan tool prove that they have the correct access rights to interact with the vehicle.").

33. [If OEMs could not require authorization to access on-board diagnostic systems, as the Data Access Law requires, they would need to remove these challenge-and-response protocols.] *See, e.g.*, June 14 Tr. 73:14-74:5 (Tierney); June 14 Tr. 113:13-114:2 (Baltes); Chernoboy Aff. ¶ 67.

34. [Importantly, these challenge-and-response protocols help protect vehicles against unauthorized changes to vehicle firmware, which would impact safety and emissions systems. Because the OEM must authorize the scan tool before the reprogramming diagnostic can be initiated, the OEM is able not only to write the "fix" but can also control its dissemination such that, when the scan tool updates the vehicle's software or firmware, it is doing so with a

manufacturer-approved fix to resolve the vehicle’s issue safely.] June 14 Tr. 73:14-74:5 (Tierney) (“with the firmware changes, the challenge response mechanism is what actually allows the reprogramming to occur” and without this mechanism “anyone could potentially update software and cause safety and emissions non-compliances”); *see also* Bort Aff. ¶ 58 (describing challenge-and-response protocol referred to as “Security Access” that unlocks the ECU before allowing firmware updates); Ex. 53 (AAI-GM-0000187) (GM presentation describing challenge and response protocol used to control access to diagnostics, including ECU reprogramming).

*Message Authentication*

35. Another security mechanism OEMs use is message authentication. Smith Aff. ¶ 154; Tierney Aff. ¶ 51; Chernoboy Aff. ¶ 53. Message authentication helps to prevent threat actors from transmitting malware or other unauthorized communications that may affect a vehicle’s core functions. Smith Aff. ¶ 155 (“Message Authentication is used to ensure that network packets originate from a valid source. The goal of message authentication is to prevent an attacker from replying or spoofing (faking) packets on a network.”); Tierney Aff. ¶ 55 (“Message authentication prevents threat actors from sending unauthorized messages to a vehicle’s safety-critical ECUs.”).

36. When an ECU transmits a message, it also sends a secure key; the receiving ECU will then verify the secure key to ensure that the message was not manipulated in any way while in transit. Tierney Aff. ¶ 54; Ex. 40 (AAI-GM-0000013). OEMs program the ECU to only receive messages with the secure key evidencing that the message is authorized and not malicious. Smith Aff. ¶ 154 (“If a packet including a data request for the vehicle to share information or perform a function is sent over a dongle, it would be rejected unless the dongle has the ability to sign the CAN packets to match the expected Message Authentication scheme.”); Tierney ¶¶ 54-55. Thus,

if the ECU message in a GM vehicle does not contain a secure key, the ECU will enter fail-safe mode. Tierney Aff. ¶ 56; Baltes Aff. ¶ 25. Fail-safe mode could mean merely ignoring the message, or instead could mean something more serious, like reducing engine power or blocking messages from that ECU for a time. *Id.* FCA employs a similar process. Chernoby Aff. ¶ 53.

37. Message authentication controls are a key design element used to protect safety features and emissions controls in vehicles. Tierney Aff. ¶¶ 52-53; Chernoby Aff. ¶ 53; Garrie Aff. ¶ 50; Smith Aff. ¶¶ 154-55.

38. Message authentication is another form of authorization that manufacturers impose on access to vehicles' on-board diagnostic systems. *See, e.g.,* Day 2 Tr. 125:15-18 (Smith) ("Q: And if the OEMs can't transfer authorization access to this third party, they would have to disable ECU or message authentication, wouldn't they? A: That's correct."). [Thus, if OEMs could not require authorization to access on-board diagnostic systems, as the Data Access Law requires, they would need to remove their message authentication controls.] *See, e.g.,* Chernoby Aff. ¶ 67 ("FCA would have to remove . . . message authentication because [it] require[s] the manufacturer to be involved in the authorization process.").

39. [Having the manufacturer as part of the "chain of authorization" for message authentication helps to ensure that unauthorized third parties cannot access, let alone change, safety and emissions-critical data in vehicle systems like acceleration, steering, airbags, and the vehicle's engine control modules. Tierney Aff. ¶¶ 52-53. Opening authentication to those outside the manufacturer's chain of authorization would increase the risks to safety and emissions controls in a number of ways—including, for instance, the ability to disable a vehicle's braking system, or control steering, while the vehicle is in motion. Tierney Aff. ¶ 94.]

*Segmentation and the Secure Gateway*

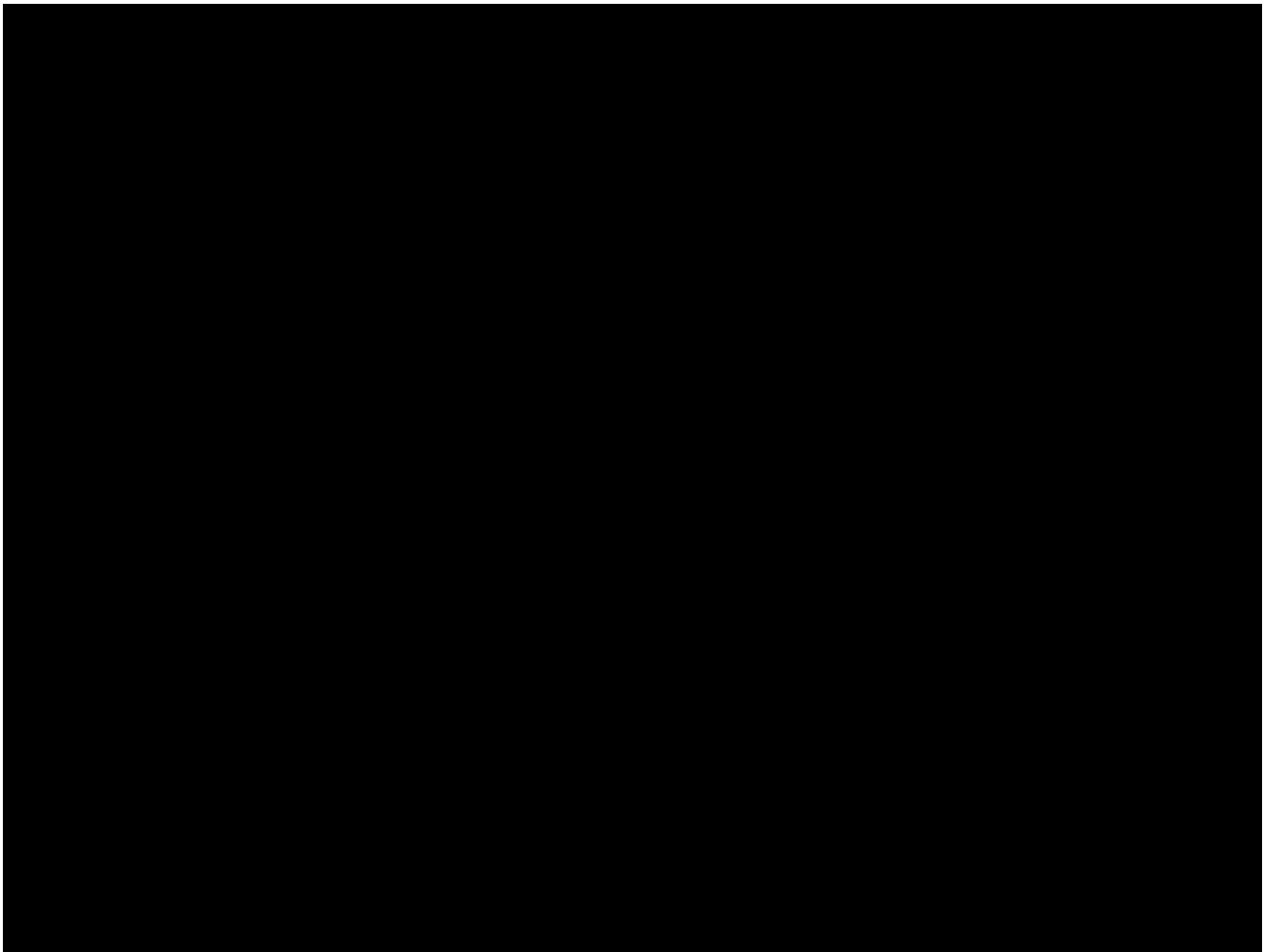
40. Another key component of cybersecurity protection is the segmentation of vehicle systems through physical isolation (using separate processors for different functions) and logical isolation (preventing direct communication between different features). Smith Aff. ¶ 75 (“Some OEMs have segmented their internal vehicle network in an attempt to keep critical systems on a separate network than their more vulnerable ECUs that have a high attack surface or have been identified during a threat assessment to have increased risk of attack.”); *see also* Tierney Aff. ¶ 57; Chernoboy Aff. ¶¶ 48-49; Garrie Aff. ¶ 60; Bort Aff. ¶¶ 42-43. Segmentation is another design element that OEMs like GM and FCA have implemented to protect safety features and emissions controls in their vehicles. June 16 Tr. 95:20-96:3 (Bort); Baltes Aff. ¶ 24; Chernoboy Aff. ¶ 48; Tierney Aff. ¶ 64; Smith Aff. ¶¶ 74-75.

41. Segmentation divides the “clean” and “dirty” sides of the vehicle. Baltes Aff. ¶ 24; Bort Aff. ¶ 85. The “dirty” side of the vehicle contains the telematics systems and other functions with external connectivity, such as the radio. On the other hand, the “clean” side is where safety and emissions critical systems reside. *Id.* OEMs implement segmentation in their vehicles through the use of separate CANs/physical isolation, firewalls, and gateway modules. Bort Aff. ¶ 86; Baltes Aff. ¶ 24; Smith Aff. ¶ 74.

42. Through physical isolation, ECUs that control safety functions are separated from connected features like the telematics system with infotainment and Bluetooth by using separate CANs. Tierney Aff. ¶ 58. For instance, as shown in the diagram below (Ex. 41, AAI-GM-0001567), in the GM Global B architecture, the electronic brake control module (“EBCM”), a safety function regulated as a Federal Motor Vehicle Safety Standard (“FMVSS”) promulgated by NHTSA, is on CAN 1. CAN 1 is connected to CAN 8 and CAN 2, both of which contain safety

components. But CAN 1 cannot communicate directly with CAN 5, which contains the telematics system. For CAN 1 and CAN 5 to communicate, the messages have to go through the central gateway. [REDACTED]

[REDACTED] . See Ex. 11 at AAI-GM-00001595-97 (providing abbreviations for ECUs); Tierney Aff. ¶¶ 28, 53, 58 (noting risk of manipulation of messages to TCM, EBCM, and ECM); Bort Aff. ¶ 93 (noting risks if ECM is successfully attacked). [REDACTED]

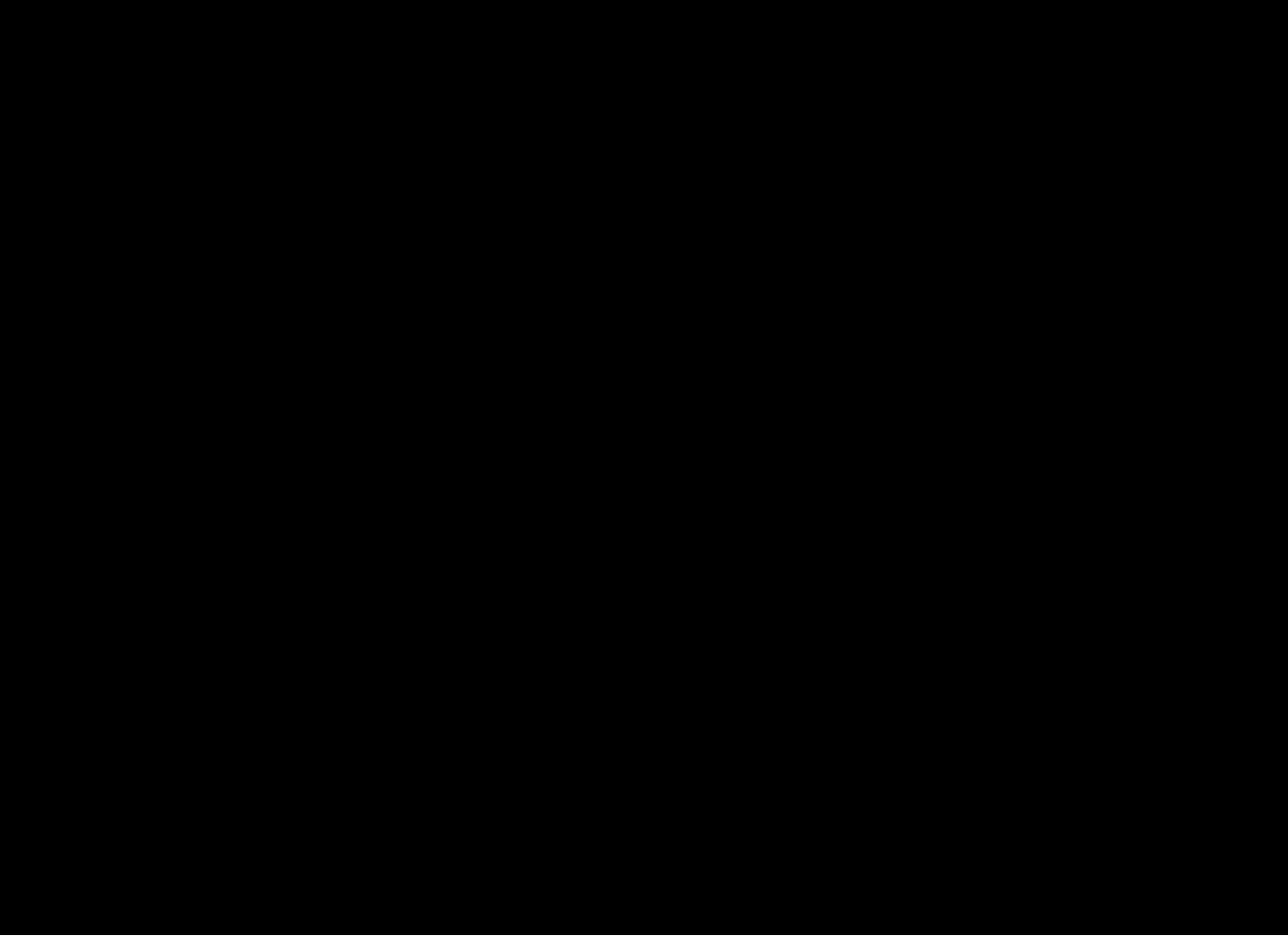


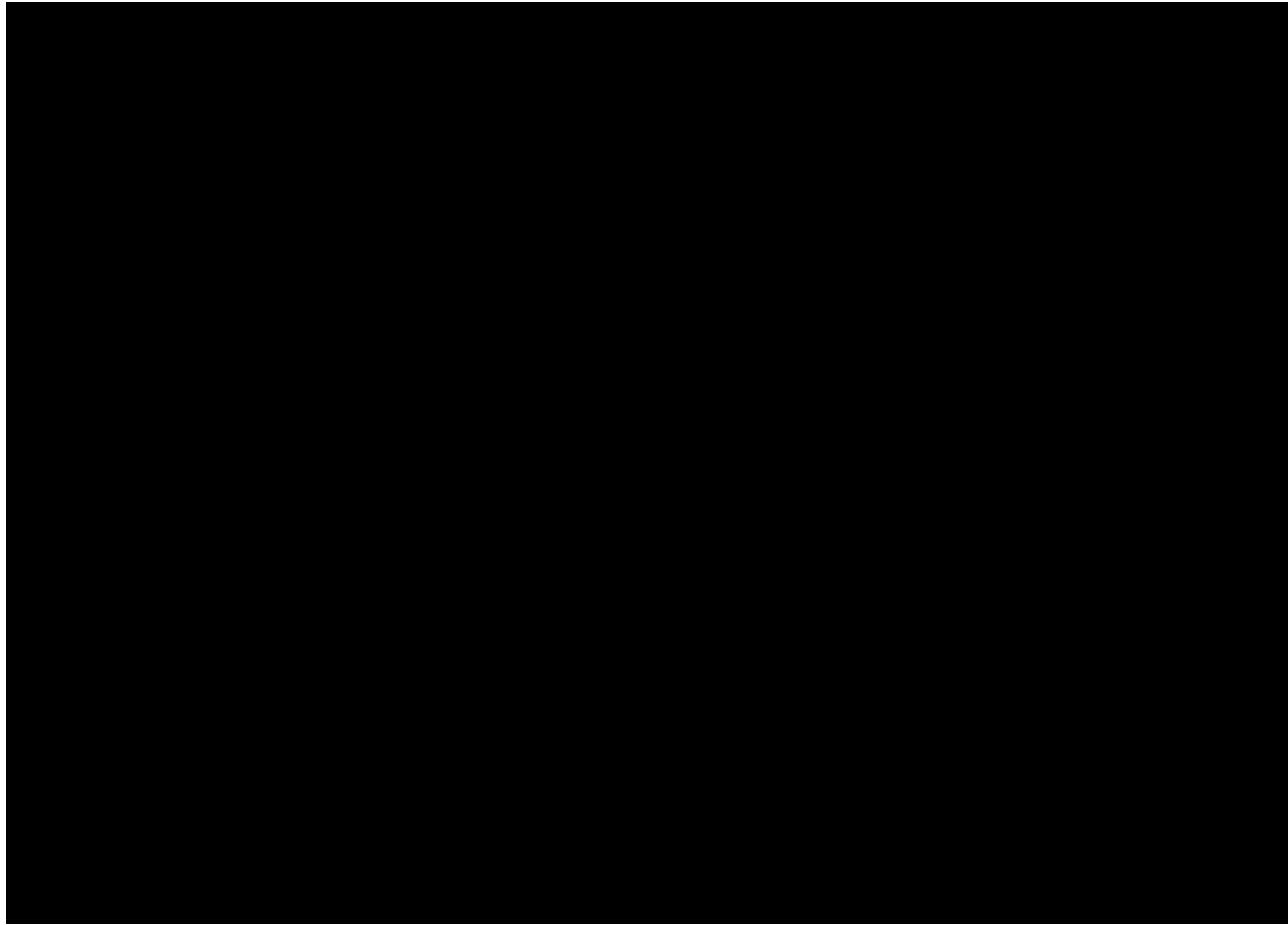
43. In the event of a security breach, this segmentation between different classes of ECUs allows manufacturers to contain the breach. Garrie Aff. ¶ 62.

44. Manufacturers also use firewalls to further separate telematics from safety features like the steering system. *See* Ex. 52 (AAI-GM-0000002) (showing placement of firewall protections); Garrie Aff. ¶ 52; Tierney Aff. ¶¶ 59-60. These firewalls help contain any security breach because breaching one firewall does not allow access to all of the vehicle's ECUs—including those that control safety-critical functions. Tierney Aff. ¶ 61.

45. For example, in the diagrams below showing the two vehicle architectures that GM currently uses, [REDACTED]

[REDACTED]. *See* Ex. 52 (AAI-GM-0000002):





46. Manufacturers use a secured gateway to control access to the CAN and the ECUs. The gateway stands as both a buffer between a vehicle's internal computer components and unauthorized external access and a barrier between functional ECU groupings. Bort Aff. ¶ 86; Smith Aff. ¶ 74. The gateway thus keeps vehicles safe from a cybersecurity standpoint. June 15 Tr. 121:24-122:1 (Smith).

47. As the diagram from Exhibit 41 above demonstrates, [REDACTED] [REDACTED] . Tierney Aff. ¶ 64. It also monitors the messages on the network and can prevent signals from going through the network if the gateway identifies unusual behavior. *Id.* ¶ 63; Baltes Aff. ¶¶ 21-23.

48. Likewise, FCA’s secure gateway divides its electrical architecture into subnetworks based on the cybersecurity risk of each function, and screens and filters messages between subnetworks. FCA also embeds an authentication code in its software. Chernoby Aff. ¶¶ 48-49. The gateway must identify this embedded authentication before the software can be downloaded to the vehicle. Chernoby Aff. ¶ 52.

49. The gateways employed by GM, FCA, and other OEMs are an additional form of authorization that manufacturers impose on access to vehicles’ on-board diagnostic systems. See, e.g., Smith Aff. ¶ 164 (“Currently, some OEMs employ a secure gateway to manage authorization of third-party tools and mechanics.”); id. ¶ 140 (“FCA documentation on the roles used to allow different levels of diagnostics access through the secure gateway indicates that these roles are validated via certificates to authorize a connected device to perform diagnostics.”).

50. If OEMs could not require authorization to access on-board diagnostic systems, as the Data Access Law requires, they would need to remove their gateways. See, e.g., June 14 Tr. 74:6-75:11 (Tierney); id. 114:19-115:1 (Baltes); id. 229:14-22 (Bort).

51. This segmentation makes it more difficult for messages—including potentially malicious messages—to travel between the different groups of ECUs and particularly protects vehicles against remote attacks through a compromised connected feature. Bort Aff. ¶ 86; Smith Aff. ¶ 74. Rather than being able directly to access a safety-related ECU via the telematics unit, a threat actor must perform a “pivot.” *Id.*; *see also* June 14 Tr. 208:5-15 (Bort). A pivot is the movement from the initial point of access to the final destination. June 14 Tr. 205:8-15 (Bort). The segmentation mechanisms OEMs employ make it nearly impossible for a threat actor to pivot through the vehicle networks from the telematics system to a safety-critical system. Bort Aff. ¶¶ 22-23, 29-31; *see also* June 14 Tr. 74:6-75:11 (Tierney) (“in our vehicles we have safety critical

control systems that support steering and braking and acceleration. But we also have connected telematics and infotainment systems that do have long-range cyber threats. So it's one of the mechanisms to keep those safety critical systems isolated from those sort of threats.”). Without segmentation, a threat actor could more easily perform a remote attack that manipulates firmware on safety-critical systems. June 14 Tr. 114:19-115:1 (Baltes).

*Firmware Encryption*

52. Manufacturers employ asymmetric encryption techniques, termed a vehicle public key infrastructure (“PKI”), to further secure the software that makes up the ECU. Smith Aff. ¶¶ 66, 151; Bort Aff. ¶ 44; Tierney Aff. ¶¶ 65-67; Baltes Aff. ¶ 15. Asymmetric encryption involves both a public and private key when the firmware is installed on a vehicle. Smith Aff. ¶ 67; Tierney Aff. ¶¶ 66-68. The public key allows third parties to verify that the software is authentic but still restricts access to the software. Tierney Aff. ¶ 68. The private key is then maintained by the manufacturer on secure servers and is required to alter the firmware. *Id.* ¶ 69. To change the firmware, the software sent to the ECU must contain the private key to verify that the software is authentic. Bort Aff. ¶ 58; Baltes Aff. ¶ 15.

53. Manufacturers are integral to the public and private key system. Without storage on a secure server controlled by the manufacturer—the entity with regulatory responsibility for maintaining safe vehicles—the private key is at risk of being compromised, undermining the entire purpose of a private key. Bort Aff. ¶ 75; Tierney Aff. ¶ 71.

54. Manufacturer control over the private keys further prevents third parties from modifying the firmware on ECUs in ways that could cause safety issues. June 14 Tr. 71:22-72:1 (Tierney); Bort Aff. ¶ 74; June 14 Tr. 115:8-116:6 (Baltes). OEMs program their vehicles to only

allow software updates that contain the private key. Bort Aff. ¶ 74; June 14 Tr. 115:8-116:6 (Baltes). The private key signifies to the ECU that the software is authentic from the OEM. *Id.*

55. Moreover, the public and private key system implicate other controls. On GM vehicles, for instance, secure boot activates any time the vehicle starts up and ensures, using the public key, that the firmware has not been modified. Tierney Aff. ¶ 72; *see also* Chernoboy Aff. ¶ 52 (describing FCA’s secure boot mechanism). Secure boot helps to ensure that the vehicle only “boots” when using software trusted by the manufacturer, as opposed to potentially corrupted software. *Id.*

56. There is good reason to include these types of protection. This vehicle firmware includes the software for important safety functions such as ABS. *See* Chernoboy Aff. ¶ 52 (firmware authentication using encryption “further secures safety-critical functions such as anti-lock braking systems (‘ABS’), steering, and acceleration.”); *see also* Tierney Aff. ¶ 70. Without ABS, a car can skid when a driver presses the brake expecting the system to prevent the wheels from locking. Tierney Aff. ¶ 70. OEMs must protect the integrity of this ABS firmware to ensure the safe operation of their vehicles. *Id.* (“If a threat actor alters firmware to disable a vehicle’s ABS, the vehicle’s safety is compromised.”); *see also* Bort Aff. ¶¶ 59-60.

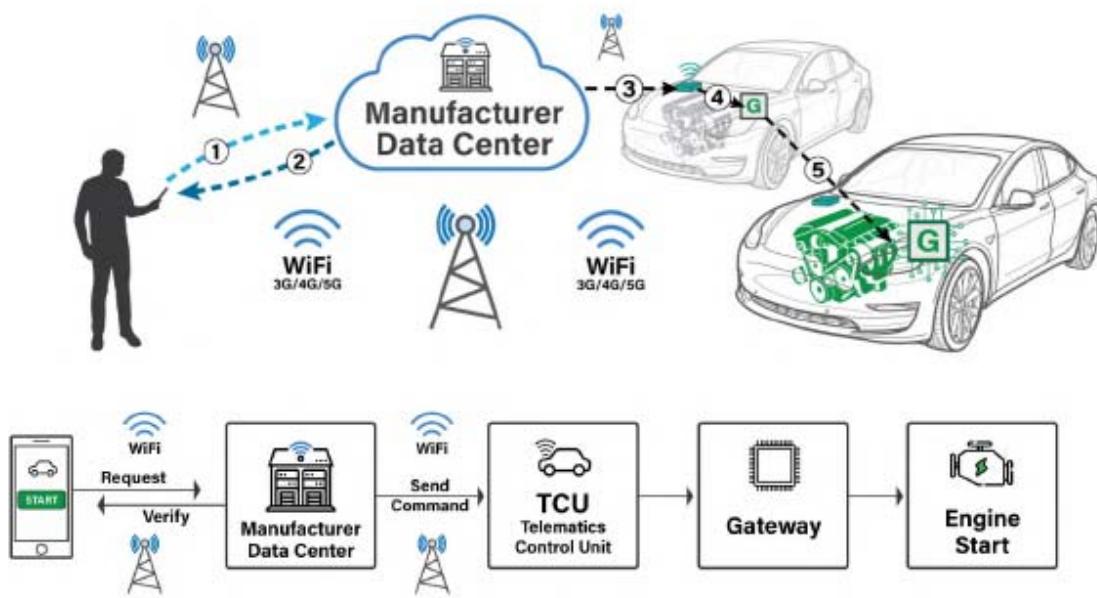
57. [Firmware encryption is a form of authorization imposed by OEMs on access to on-board diagnostic systems; thus, if OEMs could not require authorization to access on-board diagnostic systems, as the Data Access Law requires, they would need to remove their firmware encryption.] *See, e.g.*, June 14 Tr. 70:6-14 (Tierney).

58. [Further, giving others the ability to modify firmware in ways the OEM has not vetted would undermine the OEM’s vehicle design and impact safety and emissions.] June 14 Tr. 70:6-72:22 (Tierney) (describing firmware safeguards as “some of the most critical systems to

GM” because without the protections “[i]t would be disastrous . . . any third party can update software whether it’s valid from GM or not because that software could be manipulated and properties of the safety system could be changed that would cause potential safety issues for the customer, as well as emissions controls and calibrations.”); *see also* June 14 Tr. 115:20-116:12 (Baltes); Bort Aff. ¶ 74; Chernoboy Aff. ¶ 53. [Thus, as NHTSA explained in its Statement of Interest, the Data Access Law would give “uncontrolled access to vehicle firmware that executes safety-critical functions, such as steering, acceleration, and braking, which are designed in a manner that expect (and require) authenticated privileged access rights in existing implementations. Such access could allow a hacker operating remotely to access these vehicle functions, and cause a severe crash, potentially leading to deaths or serious injuries.”] Dkt. 202 at 8.

#### *Secured Communication Channels*

59. To secure vehicle telematics systems, manufacturers employ secured, encrypted communication channels. Garrie Aff. ¶¶ 58-59. For instance, at GM, when a driver uses a mobile application to communicate with the vehicle, the application sends a request through an encrypted channel to GM. Tierney Aff. ¶¶ 73-74. The GM server verifies the request and sends an encrypted message to the vehicle. *Id.* A diagram of this procedure is below:



Garrie Aff. ¶ 37.

60. To accomplish this encrypted communication, [REDACTED]

[REDACTED]  
[REDACTED] See Ex. 12 (AAI-GM-0001687). [Thus, these secured communication channels are a form of authorization that would be prohibited by the Data Access Law.]

61. [The security of the encryption key hinges on GM keeping strict control over access. Tierney Aff. ¶¶ 75, 77. If third parties had access to the encryption key, a threat actor could more easily infiltrate the vehicle's systems, including safety and emissions systems; widespread damage could result if even only one threat actor gained access to that key. *Id.* ]

### Regulatory Background

#### **A. NHTSA and the National Traffic and Motor Vehicle Safety Act**

62. NHTSA regulates, and has enforcement authority over, vehicle safety. U.S. Statement of Interest (Dkt. 202) at 2; *see also* Tierney Aff. ¶ 14; Chernoboy Aff. ¶ 16.

63. As part of its regulatory and enforcement authority under the National Traffic and Motor Vehicle Safety Act (“Vehicle Safety Act”), NHTSA publishes FMVSSs that set safety requirements for certain core vehicle functions such as acceleration, steering, and braking. U.S. Statement of Interest (Dkt. 202) at 2; *see also* Chernoby Aff. ¶ 17; Tierney Aff. ¶ 22.

64. In addition, automobile manufacturers are obligated under the Vehicle Safety Act to address safety-related defects. U.S. Statement of Interest (Dkt. 202) at 2; *see also* Tierney Aff. ¶ 16

65. [To satisfy NHTSA’s FMVSSs, a vehicle’s cybersecurity protections must be designed to ensure that its driver—not a third party or threat actor—is in control of operating the vehicle, and specifically its core vehicle functions of steering, braking and accelerating. See Tierney Aff. ¶ 23; Chernoby Aff. ¶ 18. This remains true even for those features where sophisticated computer systems now assist the driver: the driver does and must remain in control.]

66. NHTSA has issued FMVSSs that govern safety performance in vehicles. 49 C.F.R. § 571.124 (acceleration control systems), 49 C.F.R. § 571.135 (light-vehicle brake systems), 49 C.F.R. § 571.126 (electronic stability control (“ESC”—steering and anti-lock brakes); 49 C.F.R. § 571.208 (occupant crash protection—including air bags).

#### FMVSS 124 – Acceleration Control Systems

67. [To protect a vehicle’s acceleration control system, manufacturers install as an element of design in the vehicle the several layers of interdependent cybersecurity protections just discussed—including challenge and response protocols, authentication controls such as secured keys, and secured gateways that ensure the physical and logical isolation (or segmentation) of messages traveling between other ECUs and the acceleration control ECU.] Chernoby Aff. ¶¶ 19, 26; Tierney Aff. ¶ 26.

68. [Manufacturers do so in compliance with FMVSS 124 (49 C.F.R. § 571.124) to help ensure, among other things, that the driver remains in control of the vehicle's accelerator.] Chernoby Aff. ¶¶ 19, 26; Tierney Aff. ¶¶ 26, 89.

69. As discussed below, the Data Access Law would require manufacturers to disable, and thus to make inoperative, these design elements that manufacturers install in compliance with the FMVSSs to protect acceleration control devices by requiring manufacturers to remove themselves from the chains of authorization and authentication; provide standardized access to on-board diagnostic systems or vehicle networks; and provide an inter-operable, standardized, and open access platform for all vehicle data otherwise related to the diagnosis, repair, or maintenance of the vehicle. *See, e.g.*, Tierney Aff. ¶¶ 82, 97-99; Chernoby Aff. ¶¶ 65-67, 81; June 15 Tr. 122:2-16 (Smith); June 14 Tr. 249:21-250:8 (Garrie); June 14 Tr. 229:23-230:17 (Bort).

*FMVSS 135 – Light-Vehicle Brake Systems*

70. [To protect a vehicle's braking system, manufacturers install as an element of design in the vehicle several layers of interdependent cybersecurity protections just discussed—including challenge and response protocols, message authentication and other authentication controls such as secured keys, and secured gateways that ensure the physical and logical isolation (or segmentation) of messages traveling between other ECUs and the braking ECU.] *See, e.g.*, Chernoby Aff. ¶ 45; Tierney Aff. ¶¶ 41-42.

71. [Manufacturers do so in compliance with FMVSS 135 (49 C.F.R. § 571.135)] to help ensure, among other things, that the driver remains in control of the vehicle's brakes.] Chernoby Aff. ¶¶ 19, 26; Tierney Aff. ¶¶ 26, 89.

72. As discussed below, the Data Access Law would require manufacturers to disable, and thus to make inoperative, these design elements that manufacturers install in compliance with

the FMVSSs to protect light-vehicle brake systems by requiring manufacturers to remove themselves from the chains of authorization and authentication; provide standardized access to on-board diagnostic systems or vehicle networks; and provide an inter-operable, standardized, and open access platform for all vehicle data otherwise related to the diagnosis, repair, or maintenance of the vehicle. *See, e.g.*, Tierney Aff. ¶¶ 82, 97-99; Chernoby Aff. ¶¶ 65-67, 81; June 15 Tr. 122:2-16 (Smith); June 14 Tr. 249:21-250:8 (Garrie); June 14 Tr. 229:23-230:17 (Bort).

*FMVSS 135 – Electronic Stability Control*

73. [To protect a vehicle’s steering and ABS—two components of ESC—manufacturers install as an element of design in the vehicle several layers of interdependent cybersecurity protections just discussed—including again challenge and response protocols, message authentication and other authentication controls such as secured keys, and secured gateways that ensure the physical and logical isolation (or segmentation) of messages traveling between other ECUs and the ESC, steering, and ABS ECU.] *See, e.g.*, Chernoby Aff. ¶ 45; Tierney Aff. ¶¶ 41-42.

74. [Manufacturers do so in compliance with FMVSS 135 (49 C.F.R. § 571.135) to help ensure, among other things, that the driver remains in control of the vehicle’s steering and ABS.] Chernoby Aff. ¶¶ 19, 26; Tierney Aff. ¶¶ 26, 89.

75. As discussed below, the Data Access Law would require manufacturers to disable, and thus to make inoperative, these design elements that manufacturers install in compliance with the FMVSS to protect ESC—*i.e.*, steering and ABS—by requiring manufacturers to remove themselves from the chains of authorization and authentication; provide standardized access to on-board diagnostic systems or vehicle networks; and provide an inter-operable, standardized, and open access platform for all vehicle data otherwise related to the diagnosis, repair, or maintenance

of the vehicle. *See, e.g.*, Tierney Aff. ¶¶ 82, 97-99; Chernoboy Aff. ¶¶ 65-67, 81; June 15 Tr. 122:2-16 (Smith); June 14 Tr. 249:21-250:8 (Garrie); June 14 Tr. 229:23-230:17 (Bort).

*FMVSS 208 – Occupant Crash Protection*

76. [And to protect a vehicle's air bags, manufacturers install as an element of design in the vehicle several layers of interdependent cybersecurity protections just discussed—including again challenge and response protocols, message authentication and other authentication controls such as secured keys, and secured gateways that ensure the physical and logical isolation (or segmentation) of messages traveling between other ECUs and the air bags ECU.] *See, e.g.*, Chernoboy Aff. ¶ 45; Tierney Aff. ¶¶ 41-42.

77. [Manufacturers do so in compliance with FMVSS 208 (49 C.F.R. § 571.208) to ensure that the air bags only deploy when they are supposed to—in the event of a triggering accident.] Chernoboy Aff. ¶¶ 19, 26; Tierney Aff. ¶¶ 26, 89.

78. As discussed below, the Data Access Law would require manufacturers to disable, and thus to make inoperative, these design elements that manufacturers install in compliance with the FMVSSs to protect air bags by requiring manufacturers to remove themselves from the chains of authorization and authentication; provide standardized access to on-board diagnostic systems or vehicle networks; and provide an inter-operable, standardized, and open access platform for all vehicle data otherwise related to the diagnosis, repair, or maintenance of the vehicle. *See, e.g.*, Tierney Aff. ¶¶ 82, 97-99; Chernoboy Aff. ¶¶ 65-67, 81; June 15 Tr. 122:2-16 (Smith); June 14 Tr. 249:21-250:8 (Garrie); June 14 Tr. 229:23-230:17 (Bort).

*NHTSA's Regulatory and Enforcement Authority*

79. NHTSA has the statutory authority to order recalls to address unreasonable risks to motor vehicle safety. 49 USC §§ 30188-120. Of the hundreds of vehicle recalls issued each year,

auto manufacturers issue the overwhelming majority without any prompting from NHTSA. For example, in 2020, of 786 vehicle recalls, only 38—just under 5%—were influenced by NHTSA. Ex. 37 (NHTSA, *2020 Recall Annual Report* 2, [https://www.nhtsa.gov/sites/nhtsa.gov/files/documents/2020\\_nhtsa\\_recall\\_annual\\_report\\_021021-tag.pdf](https://www.nhtsa.gov/sites/nhtsa.gov/files/documents/2020_nhtsa_recall_annual_report_021021-tag.pdf).) [This percentage is so small because manufacturers do a good job of investigating and fixing issues proactively.] Chernoby Aff. ¶¶ 20-21; Tierney Aff. ¶ 16. When problem arises, NHTSA addresses safety-related concerns via direct discussion with the OEMs, often leading to the OEM issuing a “voluntary” recall. *Id.*; *see also* U.S. Statement of Interest (Dkt. 202) at 2-3. NHTSA has not ordered even a single “non-voluntary” recall in years. *Id.*

80. Moreover, OEMs have an affirmative obligation to certify the compliance of their vehicles with safety standards and recall a vehicle if they become aware of a safety-related defect. *See* U.S. Statement of Interest (Dkt. 202) at 2, 5. Thus, the Vehicle Safety Act requires OEMs act regardless of whether or when NHTSA does so. *Id.*

81. [NHTSA and auto manufacturers maintain open lines of communication.] FCA and NHTSA meet monthly. Chernoby Aff. ¶ 23. GM and NHTSA meet intermittently as well. Tierney Aff. ¶ 17. Both FCA and GM have discussed vehicle cybersecurity risks with NHTSA. *Id.*; Chernoby Aff. ¶ 23; *see generally* Exs. 6, 9, 38, 64.

82. NHTSA issues guidance documents on a wide range of topics of importance to the industry. *See* <https://www.nhtsa.gov/es/laws-regulations/guidance-documents>. [Even in areas in which NHTSA has not promulgated FMVSS or other regulations, OEMs seek to follow NHTSA’s guidance because they understand that that guidance may be a basis for NHTSA to exercise its enforcement authority to mandate a recall.] Tierney Aff. ¶¶ 18-20; Chernoby Aff. ¶¶ 24-25.

83. In 2015, for example, FCA, in coordination with NHTSA, issued a recall for over 1.4 million vehicles because a penetration test revealed vulnerabilities in vehicles' cybersecurity networks. Chernoby Aff. ¶¶ 32-33; U.S. Statement of Interest (Dkt. 202) at 6.

84. The 2015 FCA recall resulted when penetration testing identified a vulnerability in vehicle security that allowed threat actors to access the vehicles' CAN system (which system is described further above). Chernoby Aff. ¶¶ 29, 33. That access would have allowed these threat actors to gain control of the steering and braking systems. Chernoby Aff. ¶ 31.

85. At the time that vulnerability was discovered, FCA's vehicles did not employ current cybersecurity techniques. Chernoby Aff. ¶ 56. They lacked, for example, the current, isolated secure gateway (also described further above). Chernoby Aff. ¶ 48. Ultimately, in response to the vulnerability, FCA altered onboard and offboard software to make vehicles more difficult to penetrate electronically through backdoor vulnerabilities, sped up the development of an isolated secured gateway, and installed that secured gateway across its fleet. Chernoby Aff. ¶¶ 34, 49.

86. NHTSA was proactive in addressing its cybersecurity and resulting safety concerns. U.S. Statement of Interest (Dkt. 202) at 5-6; Chernoby Aff. ¶¶ 32-33. It raised those concerns with FCA before any actual harm had resulted from the safety issue. *Id.*

87. [The FCA recall definitively demonstrates that NHTSA views its recall authority as extending to cybersecurity concerns that implicate vehicle safety. U.S. Statement of Interest (Dkt. 202) at 2-3, 5-6; *see also* Tierney Aff. ¶ 14; Chernoby Aff. ¶ 28. Installing and maintaining effective cybersecurity controls around safety-critical vehicle systems is not optional. *Id.* Thus, when in 2016—the very next year after the FCA cyber recall—NHTSA issued its Cybersecurity Best Practices, auto manufacturers looked to it for guidance about what they must do to enhance

vehicle safety and reduce the risk that NHTSA would insist on a recall. Ex. 3 at 12 (NHTSA Cybersecurity Best Practices) (agency policy of reducing “unreasonable safety risks” to vehicles, drivers, passengers, and bystanders, “including those from potential cybersecurity threats and vulnerabilities.”).] GM and FCA work to ensure that their cybersecurity systems meet or exceed the standards set forth in NHTSA’s Cybersecurity Best Practices. Chernoby Aff. ¶¶ 24-25; Tierney Aff. ¶¶ 18-19.

#### **B. The Clean Air Act and the Environmental Protection Agency**

88. The Clean Air Act, initially enacted in 1963 and codified at 42 U.S.C. § 7401 *et seq.*, requires auto manufacturers to limit emissions from vehicles they manufacture. Chernoby Aff. ¶ 7; Tierney Aff. ¶ 27; Douglas Aff. ¶ 29. This requirement remains in effect for the useful life of a vehicle. Chernoby Aff. ¶ 7; Tierney Aff. ¶ 27.

89. The Environmental Protection Agency (“EPA”) requires that auto manufacturers warrant a vehicle’s emissions, which includes vehicle components that control emissions, so that any issues can be identified and remedied. Chernoby Aff. ¶¶ 8-10; Douglass Aff. ¶ 29. That identification and remediation is typically accomplished through on-board diagnostic monitoring software. Chernoby Aff. ¶ 8.

90. Before selling a vehicle, manufacturers must obtain certificates of conformity from the EPA. Chernoby Aff. ¶ 9.

91. [Manufacturers employ rigorous testing processes to ensure that vehicles they manufacture comply with EPA requirements and that such compliance will continue throughout the useful life of a vehicle.] Chernoby Aff. ¶ 10. FCA’s testing begins two to three years before it applies for an emission certification. *Id.* ¶¶ 10-11.

92. [The Clean Air Act prohibits tampering with the emissions control software in vehicles.] Chernoby Aff. ¶ 12; Tierney Aff. ¶ 28. But, unfortunately, many owners and third parties attempt to bypass anti-tampering mechanisms to try to “tune” vehicles with aftermarket software to deliver more powerful performance at the cost of higher vehicle emissions. Chernoby Aff. ¶ 12.

93. [To protect a vehicle’s emissions control systems, manufacturers install as an element of design in the vehicle the several layers of interdependent cybersecurity protections previously discussed—including challenge and response protocols, authentication controls such as secured keys, and secured gateways that ensure the physical and logical isolation (or segmentation) of messages traveling between other ECUs and the engine control module ECU.] Chernoby Aff. ¶ 13; Tierney Aff. ¶ 28.

94. [Manufacturers do so to inhibit violations of the Clean Air Act and EPA prohibitions on tampering.] Chernoby Aff. ¶¶ 8-9.

95. [As discussed in more detail below, the Data Access Law would require manufacturers to disable, and thus to make inoperative, these design elements that manufacturers install to help protect engine control modules, and thus vehicle emissions, by requiring manufacturers to remove themselves from the chains of authorization and authentication; provide standardized access to on-board diagnostic systems or vehicle networks; and provide an interoperable, standardized, and open access platform for all vehicle data otherwise related to the diagnosis, repair, or maintenance of the vehicle.] See, e.g., Tierney Aff. ¶¶ 82, 97-99; Chernoby Aff. ¶¶ 65-67, 81; June 15 Tr. 122:2-16 (Smith); June 14 Tr. 249:21-250:8 (Garrie); June 14 Tr. 229:23-230:17 (Bort).

96. Finally, problems with emissions controls can themselves lead to vehicle recalls, under the auspices of the EPA's regulatory authority. FCA has had to issue just such a recall when it was determined that vehicle emissions could exceed EPA requirements. Chernobyl Aff. ¶ 15.

### **The Massachusetts Data Access Law**

97. On November 3, 2020, Massachusetts voters passed Ballot Question 1. Douglas Aff. ¶ 4. The law that voters enacted, called here the "Data Access Law," became effective in December 2020. *Id.*; *see also* Conclusions of Law ¶ 16.

98. The Data Access Law lodges significant enforcement authority in the Attorney General. *See* Data Access Law § 5 (codified at Mass. Gen. L. ch. 93K § 6(e)); Conclusions of Law ¶ 90. [The Attorney General has reserved the right to, and intends to, exercise this authority to take action against manufacturers who fail to comply with the Data Access Law. June 25 Tr. 44:3-7 (Attorney General's counsel states: "I can say this with confidence, is that what our office wants to see happen here is get to the right answer. And so if that means threatening enforcement to move things along, maybe that's what is coming to.").]

#### **A. Existing Right-to-Repair Regime**

99. The Data Access Law includes broad data access requirements, which proponents of the law have asserted is to provide independent repair shops with data related to diagnosis, maintenance, and repair in parity with dealerships. *See* June 15 Tr. 21:10-17 (Lowe). [However, independent repair shops already had access to all data necessary for diagnosis, maintenance or repair, on the same terms as dealerships, before passage of the Data Access Law.] Baltes Aff. ¶ 26; Douglas Aff. ¶ 12; Chernobyl Aff. ¶ 57; June 15 Tr. 15:17-20 (Lowe).

100. Specifically, existing Massachusetts law required manufacturers to provide independent technicians with access to diagnostic and repair information and the ability to use the same diagnostic tools that dealers can. Douglas Aff. ¶¶ 9-10. Under a law passed in 2013 and

codified in Chapter 93K of the General Laws of Massachusetts, motor vehicle manufacturers are required, as of model year 2018, to “provide access to their onboard diagnostic and repair information system[s] . . . using an off-the-shelf personal computer with sufficient memory, processor speed, connectivity and other capabilities as specified by the vehicle manufacturer” and one of various physical interface devices, such as one complying with SAE standards J2534 or J1939. Mass. G. L. 93K(2)(d)(1). Manufacturers are further required to “provide access to the same onboard diagnostic and repair information available to their dealers, including technical updates to such onboard systems.” *Id.* Unlike the Data Access Law, Auto Innovators’ predecessor entities did not oppose the 2013 Right to Repair law, which did not create grave cybersecurity concerns, specified the standards needed to comply, and gave manufacturers four years to implement changes. Douglas Aff. ¶ 11; June 16 Tr. 92:5-93:9 (Smith); June 16 Tr. 97:2-6 (Bort).

101. Further, auto manufacturers, through their trade associations, entered into a memorandum of understanding (“MOU”) in 2014 under which they agreed to provide that same access and information on the same terms in all fifty states and the District of Columbia. [Manufacturers comply with that law and the MOU.] Douglas Aff. ¶ 12. This means that an independent repair shop has the opportunity to have the tools at its disposal to repair vehicles—just like any OEM dealership. June 15 Tr. 15:17-20 (Lowe).

#### **B. ACA’s Drafting of and Campaign for the Data Access Law**

102. After reaching agreement on the MOU, the Auto Care Association (“ACA”), a group composed of organizations and individuals involved in aftermarket parts and services, began to petition for additional access to vehicle data, including telematics data. *See* June 15 Tr. 17:8-18:1 (Lowe) (describing efforts after 2014 regarding access to telematics data). ACA then drafted and campaigned for the petition that is now the Data Access Law. June 15 Tr. 13:6-12, 18:9-21:6

(Lowe) (testifying that ACA drafted the ballot initiative and contributed to the over \$20 million campaign to pass the initiative),

103. ACA intended for the Data Access Law to expand the scope of the existing Right to Repair Law dramatically. For instance, ACA drafted the definition of “mechanical data” in Section 1 of Data Access Law to include data “otherwise related to the diagnosis, repair, or maintenance of the vehicle” to ensure the law adopted a broad, “catch-all” interpretation of the data OEMs must provide. *See* June 15 Tr. 24:3-6 (Lowe). ACA intended the law to require that such mechanical data be directly transmitted between the vehicle and an owner’s mobile phone—a point the Attorney General confirmed in the voter guide it sent to Massachusetts voters. June 15 Tr. 29:6-30:2 (Lowe); Ex. 509 at 4 (“Owners of motor vehicles with telematics systems would get access to mechanical data through a mobile device application.”). Additionally, ACA intended Section 2 to prohibit OEMs from managing access to vehicles and require a standardized system for authorization. June 15 Tr. 24:7-25:3, 26:13-17 (Lowe). In Section 2, ACA included a requirement for access to “vehicle networks,” which it understood to extend beyond on-board diagnostic systems. June 15 Tr. 66:10-67:5. (According to Aaron Lowe, ACA wanted to ensure that the law would cover certain electric vehicles that do not have on-board diagnostic systems (*id.*), but the Data Access Law does not contain any limitation surrounding application to only electric vehicles.)

104. When ACA proposed the ballot initiative, ACA was aware of the OEMs’ cybersecurity concerns related to this expansion in access to data. *See* June 15 Tr. 21:20-22:2 (Lowe) (describing discussions with OEMs about cybersecurity concerns). ACA also knew that the systems needed to comply with the Data Access Law—including a standardized authorization system, a third party needed to manage that authorization system, and an interoperable,

standardized, open-access platform—did not exist. *See* June 15 Tr. 24:24-26:7 (Lowe) (testifying that no standardized authorization system exists); June 15 Tr. 13:20-22 (Lowe) (testifying that he is not aware of any OEM with an interoperable, standardized, and open access platform); June 15 Tr. 27:16-18 (Lowe) (testifying that the third party needed to manage authorization does not exist).

105. Despite this knowledge, ACA decided on effective dates for the Data Access Law that it knew made compliance impossible. *See* Ex. 62 at AAI-ACA-0038565-68 (noting that OEMs are unlikely to be able to meet the deadlines in the law but opposing extending the timeline); June 15 Tr. 30:16-19 (Lowe) (“Q: Section 3 is effective with model year 2022? A: That’s what it says, yes. Q: And you were involved in picking that day, weren’t you? A: I was one of the group of people involved yes.”). Indeed, ACA considered allowing longer time periods for compliance with the law to give manufacturers sufficient time to try to comply, but ACA’s CEO, Bill Hanvey, was “fundamentally opposed to initially conceding these time frames to the auto makers” because “[t]iming is [ACA’s] ultimate bargaining chip.” Day 2 51:9-53:3; Ex. 62 at AAI-ACA-0038568.

106. ACA also encouraged passage of the Data Access Law with knowledge that the cybersecurity measures that OEMs would be forced to remove from their vehicles would need to be replaced. Indeed, ACA prepared and reviewed a business plan that would charge regular fees to Massachusetts drivers to sustain an entity that would manage cybersecurity for vehicles in the Commonwealth—a plan that would create “an extremely profitable return for investors” in that entity. June 15 Tr. 53:13-54:9; Ex. 62. Under that plan, ACA expected fees exceeding “\$4 billion per annum by 2033.” June 15 Tr. 56:13-57:13; Ex. 68. None of this plan was disclosed to the voters. *See* June 15 Tr. 54:3-5 (Lowe)

### C. Effect of Section 2

107. Section 2 of the new law requires one of two things. Either manufacturers must immediately make OBD systems “standardized” and accessible “without authorization by the manufacturer, directly or indirectly.” Data Access Law § 2 (codified at Mass. Gen. L. ch. 93K, § 2(d)(1)); Conclusions of Law ¶¶ 55, 62, 63. Or they must design and implement an “authorization system for access to vehicle networks and their on-board diagnostic systems [that] is standardized across all makes and models sold in the Commonwealth and . . . administered by an entity unaffiliated with a manufacturer.” *Id.* [Either way, then, manufacturers are cut out of the process. *Id.*]

#### *Section 2 Requires Removal of Cybersecurity Controls that Authorize Access to On-Board Diagnostic Systems*

108. [Currently, OEMs limit authorization to access certain diagnostics through the OBD-II port.] *See, e.g.*, Smith Aff. ¶¶ 141, 164 (identifying the secure gateways, ECU authentication, and message authentication as authorization mechanisms OEMs use to limit access to data necessary for diagnostics, maintenance, and repair); June 16 Tr. 94:6-22 (Garrie) (explaining that Toyota does not permit third parties to write their own software to ECUs, rather a third party is only authorized to install software downloaded from the Toyota website after agreeing to Toyota’s terms of use); Bort Aff. ¶ 54 (“OEMs employ various authorization mechanisms before providing access to certain sensitive diagnostic data and functions through the OBD system.”); June 15 Tr. 197:10-13 (Romansky) (testifying that he is not aware of any manufacturers that have removed themselves from the authorization process for accessing OBD systems.).

109. [Section 2’s requirement for manufacturers to remove themselves from the process of authorizing access to the diagnostic system means that manufacturers would no longer be able

to employ necessary cybersecurity features—including challenge-and-response protocols, message authentication, segmentation and secure gateways, and firmware encryption techniques.]

June 14 Tr. 119:2-4 (Baltes) (“we have authorization throughout all of our security controls to ensure the safety of our customers”); *see also* Smith Aff. ¶ 141 (stating that OEMs could only retain firmware encryption and message authentication if “the authorization aspects of these security measures are administered by an entity unaffiliated with an OEM”); June 15 Tr. 125:15-18 (Smith) (“Q: And if the OEMs can’t transfer authorization access to this third party, they would have to disable ECU or message authentication, wouldn’t they? A: That’s correct.”); June 14 Tr. 249:21-250:8 (Garrie) (testifying that OEMs must remove the secure gateway, challenge and response protocols, and wireless communication controls); June 14 Tr. 113:5-22 (Baltes) and June 14 Tr. 73:14-74:5 (Tierney) (testifying that GM would have to disable its challenge and response protocol); June 14 Tr. 70:6-72:3 (Tierney) and June 14 Tr. 115:20-116:12 (Baltes) (testifying that GM must remove its firmware safeguards to comply); June 14 Tr. 74:6-75:11 (Tierney) (“no authorization and full access to vehicle networks, we would have to remove the gateway and the firewall to provide that access”); Day 1, 229:3-22 (Bort) (testifying that OEM’s secure gateway “wouldn’t be able to function in the exact same manner of preventing – of managing authorization”).

110. [Manufacturers’ challenge-and-response protocols, for example, rely on the manufacturer’s involvement; without the challenge-and-response protocol, a threat actor could gain access to diagnostics controls and reprogram safety ECUs and emissions systems.] June 14 Tr. 113:5-22 (Baltes) (“Q: If GM is not permitted to require direct or indirect authorization to its vehicles onboard diagnostic systems, could GM keep its secure unlock protection [a challenge and response protocol]? A: No. . . only the GM back office has the secrets and authorization to generate

the correct response to the challenge, which is sent back via the tool and matches it with the ECU.”); June 14 Tr. 73:14-74:5 (Tierney) (removing challenge and response protocols would be “very detrimental to the security of our vehicles and the safety of the customer because . . . anyone could potentially update software and cause safety and emissions non-compliances.”); Bort Aff. ¶¶ 58-59; Chernoby Aff. ¶ 67.

111. [Similarly, the encryption techniques used to secure ECU firmware changes (also referred to as firmware safeguards, PKI, and secure programming) are inextricably tied to the OEMs. Manufacturers hold the private keys that are required to alter the firmware.] Tierney Aff. ¶ 69. Without the private key, the ECU will reject an attempt to change its firmware. *Id.*; Bort Aff. ¶ 58; Baltes Aff. ¶ 15. [Accordingly, by controlling the ability to include the private key on a firmware update, OEMs must authorize any modifications to firmware for change to be implemented. *Id.*]

112. Currently, if a franchised dealer or independent repair facility wishes to update the software on a vehicle, it can do so through the OBD port, so long as the manufacturer authorizes the software update. Chernoby Aff. ¶ 38; Tierney Aff. ¶ 39; Garrie Aff. ¶ 31; June 15 Tr. 82:23-83:12 (Lowe); Smith Aff. ¶ 142. [Without these authorization protections, threat actors acting intentionally—or even independent car enthusiasts tinkering with their vehicles acting unintentionally—could install malicious software or send unauthorized messages to vehicles, compromising safety-critical vehicle systems.] Bort Aff. ¶¶ 59-60; June 14 Tr. 116:21-117:10 (Baltes); June 14 Tr. 71:22-72:3 (Tierney); Tierney Aff. ¶ 94; Chernoby Aff. ¶¶ 71, 73; Garrie Aff. ¶¶ 86-87. [For example, if a tool attached to the OBD port is itself corrupted with malware, that tool malware can be transmitted and written onto the vehicle, thereby potentially compromising core safety and emissions functions.] See Garrie Aff. ¶¶ 76-78.

*Manufacturers Cannot Currently Comply with Section 2*

113. [There is no current way to comply with the requirements in Section 2.] *See, e.g.*, June 14 Tr. 118:23-25 (Baltes) (“Can GM comply with section 2 of the Data Access Law today? A: No. Not while keeping our customers safe, no.”); June 14 Tr. 56:3-56:5 (Tierney) (“Q: Do you believe that GM could comply with the Data Law? A: Not and meet our obligations to protect the security of our vehicles and the safety of our customers.”); June 15 Tr. 193:24-194:25, 197:10-13 (Romansky) (stating that not aware of an OEM that has tested or implemented any of the proposed solutions to address access to diagnostics).

114. [Because manufacturers require authorization to vehicles’ on-board diagnostic systems to ensure the safety of their vehicles,] the alternative compliance option in Section 2 mandates that “the authorization system for access to vehicle networks and their on-board diagnostic systems” be “standardized across all makes and models sold in the Commonwealth” and “administered by an entity unaffiliated with the manufacturer.” Data Access Law § 2. But doing so is impossible as no such third party or standardized authorization systems exist. *See, e.g.*, June 15 Tr. 27:16-18 (Lowe) (testifying that third party required to manage authorization does not exist); June 15 Tr. 97:1-7 (Potter) (same); June 15 Tr. 125:6-9 (Smith) (same); June 15 Tr. 25:9-26:7 (Lowe) (testifying that he is not aware of any standardized authorization system); June 15 Tr. 101:8-16 (Potter) (stating that no standardization across secure gateways that OEMs use to manage access to vehicle systems); Smith Aff. ¶¶ 49, 51, 125-26, 147 (noting differences in diagnostic information provided by OEMs and acknowledging “gap in standardization” for “diagnostics information and repair methodologies”); Ex. 27 at 3 (Def.’s 2d Suppl. Resp. to Pl.’s 1st Set of Requests for Admission (Apr. 30, 2021)) (“[T]he Attorney General further states that she is not aware of any existing ‘authorization system for access to vehicle networks and their on-board

diagnostic systems’ that is ‘standardized across all makes and models sold in the Commonwealth and is administered by an entity unaffiliated with a manufacturer.””).

115. At trial, Lowe testified that ACA was working with the Equipment Tool Institute (“ETI”) to “develop” an entity that could serve as the unaffiliated entity contemplated by Section 2 of the Data Access Law. June 15 Tr. 38:25-39:5 (Lowe). But Mr. Potter, the Chief Technology Officer of ETI, testified that ETI currently has three employees—one of whom is an event planner, and none of whom have any cybersecurity expertise. June 15 Tr. 92:3-21 (Potter). ETI is not capable of serving as the unaffiliated entity that is described in Section 2 of the Data Access Law. June 15 Tr. 97:8-11. ETI does not have any system in place to run background checks to accredit independent repair facilities. Nor does ETI have the capability to have anything to do with the security of the platform that the Data Access Law contemplates. June 15 Tr. 98:10-18 (Potter).

116. Likewise, “vehicle networks” encompass all of the electronic networks of a vehicle, including CAN buses connecting ECUs. Bort Aff. ¶ 62; Garrie Aff. ¶ 67; June 15 Tr. 186:10-187:1, 187:5-22 (Romansky) (testifying that vehicle networks serve a different role than on-board diagnostics systems, that vehicle networks encompass “a communication within a vehicle,” that there may be “multiple vehicle networks” in a vehicle, and that those networks “might include, for example, the internal systems of the vehicle that control powertrain”); June 15 Tr. 124:5-19 (Smith) (“vehicle networks” means “the network between the ECUs, the components inside the vehicle and the OBDs attached to that as well”; “Q: The entire network? A: Yes, the entire car network, the one in the car.”). These networks vary between manufacturers within the Commonwealth, and [access to those networks is not at all standardized. ] See Bort Aff. ¶ 64; June 15 Tr. 101:3-11 (Potter).

*Attempts to Comply with Section 2 Would Undermine Vehicle Safety and Emissions Integrity*

117. [Without a standardized and third-party option for maintaining authorization mechanisms, OEMs must disable these access controls to attempt to comply with Section 2, which would trigger a substantial, and dangerous, change to vehicle cybersecurity protections.] June 14 Tr. 71:22-72:3 (Tierney); Tierney Aff. ¶ 94; Chernoby Aff. ¶¶ 71, 73; Garrie Aff. ¶¶ 86-87; Bort Aff. ¶ 60.

118. [Even if an unaffiliated entity required under Section 2 existed (and it undisputedly does not), the risk to vehicle safety and emissions integrity would be far greater if the manufacturer is no longer allowed to authenticate users and control access to vehicle systems and an unknown and unidentified third party assumes that role. Removing the manufacturer would be removing the one entity best able to develop, test, certify, and securely deploy any software updates.] June 14 Tr. 70:3-5 (Tierney) (“we [GM] are uniquely positioned for understanding how our safety systems work and insuring that the right software goes to the right ECU at the right time.”); *see also* Bort Aff. ¶ 74; Chernoby Aff. ¶¶ 68-69, 76; Tierney Aff. ¶ 94. ] June 14 Tr. 69:2-19 (Tierney) (“firmware changes obviously go through an in-depth development process . . . it’s done that way for two reasons. One is there’s an extremely high number of software across all of our various ECUs and in vehicles globally. So there’s a tremendous amount of software to manage, and this software is vitally important to the safety of the vehicle. . . the software controls those safety critical systems . . . So it’s important that we maintain and understand what software goes where so that our customers get the right software at the right time.”); *see also* Tierney Aff. ¶¶ 108-110.

119. [Manufacturers also are uniquely well suited to prevent cybersecurity attacks because they are the ones ultimately responsible for the safety of their vehicles—from a regulatory, products liability, and a brand-image perspective. June 14 Tr. 70:3-5 (Tierney); Bort Aff. ¶ 74;

Chernoby Aff. ¶¶ 68-69, 76; Tierney Aff. ¶ 108-110. No one understands the intricacies of a given manufacturer's vehicle systems better than the manufacturer itself. *Id.* Removing manufacturers from the chain of authorization would greatly increase the risk that a threat actor could gain access to a vehicle and alter its safety- and emission-critical vehicle data.] June 14 Tr. 71:22-72:3 (Tierney); Tierney Aff. ¶ 94; Chernoby Aff. ¶¶ 71, 73; Garrie Aff. ¶¶ 86-87; Bort Aff. ¶ 60.

120. [Given that vehicle safety is at issue, the public consequences of allowing Section 2 of the Data Access Law to take effect are significant.] See, e.g., June 14 Tr. 89:2-90:4 (Tierney) (describing the example of the impact of complying with the Data Access Law on the protections surrounding and safety of braking systems); June 14 Tr. 115:20-117:10 (Baltes) (explaining that without authorization protections “someone is able to reprogram software in the ECU, he or she has complete control over what that ECU can do, including removing security controls and removing functions that impact safety and emissions” and that any remaining security checks, like rationality checks, would not fully protect the vehicle “making it a lot easier for an adversary to have a successfully attack.”); [U.S. Statement of Interest (Dkt. 202) at 6 (“DOT is concerned that the Data Law potentially creates a similar serious cybersecurity risk to motor vehicle safety by effectively requiring open remote access to certain vehicle systems through the removal of existing manufacturer access controls.”).]

#### **D. Effect of Section 3**

121. [Section 3 of the Data Access Law, in turn, requires that any vehicle, starting with model year 2022, that uses telematics must use an “inter-operable, standardized and open access” platform that is accessible to the owner and third-party repair shops without authorization from the manufacturer.] Data Access Law § 3 (codified at Mass. Gen. L. § 2(f)); Conclusions of Law ¶¶

74-87. [Coupled with Section 2's requirement for ungated access to OBD systems—which applies to vehicles with model years 2018 and onward—Section 3 mandates that the “open access” platform be accessible without any manufacturer authorization.] *Id.* The Data Access Law further requires that manufacturers provide an inter-operable, standardized, open access platform that (1) is capable of securely communicating all mechanical data—*i.e.*, all data “otherwise related to” vehicle diagnosis, maintenance, and repair, including telematics data—via direct connection to the platform; (2) is directly accessible by the vehicle owner through a mobile-based application; (3) is directly accessible by independent repair facilities; and (4) provides independent repair facilities with the ability to send commands to in-vehicle components. *Id.*

*Manufacturers Cannot Currently Comply with Section 3*

122. [There is no current way to comply with the requirements of Section 3.] June 16 Tr. 41:11-42:10 (all of the parties’ experts agreeing that no OEMs could meet the requirements of the Data Access Law).

123. No platform or mobile-based application required to comply with the Data Access Law currently exists. June 15 Tr. 126:3-15 (Smith) (“Q: So you don’t know of any OEM that has an interoperable standardized open access system? A: I do not. Q: And you don’t know of one even being tested? A: Correct.”); June 15 Tr. 13:20-22 (Lowe) (“Q: Can you identify a single OEM that has an interoperable standardized open access platform? A: No.”); Garrie Aff. ¶ 107 (“Based on my industry knowledge, interviews, and materials considered in preparing this affidavit, no inter-operable, standardized, and open access platform currently exists to comply with the Data Law’s requirements.”); *see also* June 15 Tr. 30:8-15 (Lowe) (third-party entity does not exist); June 15 Tr. 69:9-17 (Lowe) (standardized system does not exist); June 15 Tr. 95:21-96:17 (Potter) (mobile-based application contemplated by Section 3 of the Data Access Law does not exist); June 15 Tr. 205:20-206:1 (Romansky) (standardized system does not exist).

124. No platform compliant with the Data Access Law's requirements can be securely developed in time to comply with that law because the design and validation of model year 2022 vehicles was already completed, the vehicles are in production, and many are now close to being shipped to dealerships in Massachusetts and elsewhere. Tierney Aff. ¶7; Chernobyl Aff. ¶ 6; Garrie Aff. ¶ 108; Bort Aff. ¶¶ 92-93. Even if such a system could be designed in a manner that reduced or eliminated cybersecurity risk, it would take at least five years to do. See June 14 Tr. 200:20-201:8, 232:12-233:5 (Bort) (noting that it takes years to make changes to vehicle architectures, and expecting the process of developing a solution to take at least five years); June 14 Tr. 80:11-81:14 (Tierney) (describing steps to develop a solution and estimating the process to require at least seven years); June 14 Tr. 250:9-17 (Garrie) (approximately three to eight years); June 15 Tr. 180:14-184:23 (Romansky) (describing recommended steps before implementing a change to a vehicle). And for large-scale electrical architecture redesigns, manufacturers must design, test, validate, and implement any design change in such a way that it ensures the change works as intended, does not compromise any other component of the vehicle architecture, and does not increase the system's vulnerability to attacks in unintended ways. June 14 Tr. 200:20-201:8 (Bort); Garrie Aff. ¶ 123; Bort Aff. ¶ 91; June 15 Tr. 128:17-128:24 (Smith) (acknowledging that "creating the platform required by section 3 will take time to design, test and validate"); June 15 Tr. 180:14-185:1 (Romansky) (testifying that even minor changes to vehicle software could have unintended consequences impacting driver safety, so software changes must be subject to vigorous testing and validation, and describing recommended steps before implementing a change to a vehicle).

*Disabling Telematics Is Not a Solution*

125. As no compliant solution currently exists, the Attorney General and one of her experts have suggested that OEMs can "comply" with Section 3 of the Data Access Law simply

by disabling telematics systems. *See, e.g.*, Attorney General's Post-Evidence Memorandum (Dkt. 217) at 12; Smith Aff. ¶ 78.

126. [But disabling telematics systems would not be an act taken in compliance with the law's requirements—which are to create an inter-operable, standardized, and open access platform. Data Access Law § 3 (codified at Mass. Gen. L. § 2(f)); *see also, e.g.*, June 15 Tr. 31:12-15 (Lowe) (“Q: But turning off the telematics system doesn’t create an interoperable standardized open access platform on the vehicle, does it? A: No.”). Rather, it would be a workaround to try to avoid those requirements by not falling under the law’s terms. *See* June 15 Tr. 117:6-9, 135:14-17 (Smith) (conceding that turning off telematics systems is “more like exempting out” because “[y]ou’re just not going to participate until you get to that point.”); June 15 Tr. 32:9-12 (Lowe) (“Q: Did your side tell Massachusetts voters that a vote for the Data Access Law was a vote against the telematics systems that they signed up for with their auto manufacturer? A: I don’t believe so.”). Saying that manufacturers could “comply” with Section 3 by removing their telematics systems is no different than saying that manufacturers could do so by deciding not to sell vehicles in the Commonwealth at all. *See* Conclusions of Law ¶ 84.]

127. Disabling telematics systems would remove safety features such as FOTA updates that facilitate maintaining vehicles in a safe condition. Bort Aff. ¶ 96; Garrie Aff. ¶ 100; Chernobyl Aff. ¶ 83; Tierney Aff. ¶ 112. Over-the-air updates have become particularly important ways to update vehicle software, including updates that impact safety and emissions systems. Bort Aff. ¶¶ 97-98; Garrie Aff. ¶¶ 101-102; Chernobyl Aff. ¶ 83. Disabling telematics systems would also remove a myriad of other safety features, such as emergency crash notification, which notifies authorities and first responders when a vehicle has been in an accident. Bort Aff. ¶ 96; Garrie Aff. ¶ 100. Moreover, autonomous vehicles in particular depend on telematics systems for safety-

critical functions like steering because the systems are intertwined with the functions themselves.  
Chernoboy Aff. ¶ 83. Voters were not told prior to the election that compliance with the Data Access Law was impossible and that therefore OEMs would have to disable telematics (and not offer for sale the related telematics-enabled safety features) on all cars sold in the Commonwealth for the foreseeable future.

128. Indeed, even the Attorney General's expert admits that turning off telematics systems would remove manufacturers' ability to send FOTA updates to vehicles and remediate potential safety risks. June 15 Tr. 118:14-21 (Smith). FOTA is the best way to update vehicles and makes recalls easier, and without FOTA updates owners who do not bring in their vehicles for traditional recall repairs would be at a safety risk. Bort Aff. ¶¶ 97-98; Chernoboy Aff. ¶ 83; Tierney Aff. ¶ 112. Moreover, disabling telematics systems would inhibit manufacturers from detecting potential safety risks before they manifest—by, for example, disabling intrusions detection systems that communicate to the manufacturer the presence of a hack or malware introduced to the vehicle via a physical connection as well as limiting manufacturers' ability to collect data to assess malfunctioning components. Garrie Aff. ¶¶ 104-105.

129. Finally, there is no reason to believe that disabling telematics systems could be cabined just to Massachusetts, at least as to aftermarket sales. Tierney Aff. ¶ 111 (“It is a practical impossibility to disable telematics systems for all vehicles that might one day be resold in the Massachusetts aftermarket.”); Garrie Aff. ¶ 99 (“It is also unclear at best whether disabling telematics could be cabined to just Massachusetts, especially for aftermarket sales. . . disabling telematics would effectively create a nationwide change to ensure avoidance of the Data Law.”).  
[That Data Access Law avoidance method would effectively require a nationwide change, which

would implicate other constitutional concerns, see Conclusions of Law ¶¶ 86-87 (discussing Massachusetts's inability to regulate out-of-state commerce).]

*The Attorney General's Proposed Long-Term Solutions for Compliance Do Not Work*

130. The Attorney General's experts' proposals for "medium" and "longer-term" solutions for OEMs to develop are flawed.

131. Secure Vehicle Interface ("SVI") is not a viable solution for complying with the Data Access Law's requirements. No SVI system currently exists in any motor vehicle sold in the Commonwealth, much less one that is standardized across all makes and models sold in the Commonwealth. June 15 Tr. 200:8-14 (Romansky) (stating that not aware of any OEMs that have implemented SVI); June 15 Tr. 102:9-17 (Potter) (testifying that SVI has not been used by an OEM for diagnostics, and implementation would require a number of development steps); June 15 Tr. 38:17-20 (Lowe) (testifying that he is not aware how long it would take OEMs to reprogram their vehicles to implement SVI); Garrie Aff. ¶ 112; Bort Aff. ¶ 111. GM has evaluated the SVI framework in the past, and found it not to be a secure solution. See June 14 Tr. 79:2-8 (Tierney). [NHTSA also expressed concerns about the feasibility of the SVI given the challenges of establishing a certificate authority.] Ex. 64; June 15 Tr. 34:5-13 (Lowe) ("the establishment of a certificate authority would be extremely difficult and, in their opinion, likely not possible.").

132. Having a third party manage public key infrastructure ("PKI") as part of a Secure Credential Management System ("SCMS") is likewise not a viable path to compliance with the Data Access Law's requirements.

133. To start, SCMS has never been used to provide access to diagnostics and repair data or at the scale required for compliance with the Data Access Law. June 15 Tr. 192:24-193:5 (Romansky) ("I'm not aware of the use for transmitting diagnostic data."); Bort Aff. ¶ 112.

134. Additionally, PKI would be an authorization system run by a third party. No such third party presently exists that could manage this PKI. June 15 Tr. 30:8-15 (Lowe) (testifying that he is not aware of existing third party entity to manage certificates); *see also* June 15 Tr. 97:1-7 (Potter); June 15 Tr. 125:6-9 (Smith). [Existing third-party authorization systems allow auto manufacturers to be involved in the authorization process.] *See* Chernoboy Aff. ¶ 75 (describing FCA's controls over AutoAuth). [Allowing manufacturers to be involved in the authorization process reduces the opportunity for threat actors to make critical changes to safety- and emissions-related vehicle data that could allow them to take remote control of a vehicle.] *Id.*; *see also* June 14 Tr. 116:21-118:18 (Baltes); June 14 Tr. 266:12-22 (Garrie); June 14 Tr. 72:4-25 (Tierney).

135. [Existing third-party attempts to set up and regulate platforms show the difficulty of making such a system secure.] For instance, the National Automotive Service Task Force (“NASTF”)'s efforts to establish an independent process for managing locksmiths' and independent repair shops' access to vehicle keys took years and was repeatedly re-launched due to security issues. *See* June 14 Tr. 27:24-29:11 (Douglas).

136. NASTF facilitates a dialogue between manufacturers and technicians. *See* Douglas Aff. ¶ 15. NASTF led the creation of what is called the secure data release model (“SDRM”) program. Douglas Aff. ¶ 24. The SDRM program is a voluntary project between manufacturers and locksmiths, run by NASTF. *Id.* ¶ 16. Launched after five to six years of development, through SDRM, NASTF verifies that locksmiths and independent repair shops have background checks, insurance, and are licensed repair shops or locksmiths. *Id.*; June 14 Tr. 27:24-28:1 (Douglas). Manufacturers can then use that information when deciding whether to release codes to technicians to allow them to complete repairs. Douglas Aff. ¶ 16. For instance, a vehicle key fob comes with a transmitter that sends a signal to unlock and start the vehicle. *Id.* ¶ 17. In order to repair or

replace the key, the aftermarket locksmith needs to know what the signal is. *Id.* But the manufacturer needs to make sure that the signal does not go out to just anyone, so NASTF set up this system to verify the identity of the locksmith. *Id.* ¶¶ 18-21. Importantly, in this verification process, the OEM maintains sole control over its data (here, the signal necessary for a fob to unlock a vehicle's door); NASTF never possesses or controls that data. June 14 Tr. 27:6-22 (Douglas) (“Q: Like the immobilizer code or the key code. Do they hold any of the OEM’s data? A: No. We could not. I mean, that would be, you know, 280 million vehicles on the road . . . . there’s just no possible way that NASTF could maintain that kind of security or that kind of data.”)

137. There were several security concerns with the SDRM, and it has been repeatedly relaunched with additional security measures such as encrypted passwords, stronger password requirements, and algorithms in the background to track unusual behavior. June 14 Tr. 27:24-29:11 (Douglas). And that is just for key fobs. Even the Data Access Law’s proponents concede that SDRM is not a workable solution to that law, involving as it does a much more limited set of data than the data access required under the Data Access Law. June 15 Tr. 78:5-10 (Lowe) (“Q: And you acknowledge yourself while SDRM resolves a key code issue, that’s a more limited set of data than what we’re dealing with in this case, right? A: Yeah, you’re just talking about a key code. You’re not talking about the breadth of diagnostic repair information that would need to be provided under the Data Access Law.”).

138. [The opinions of the Attorney General’s expert that compliance with the Data Access Law is possible in the “medium” term also hinge on an incorrect definition of the vehicle data covered by the Data Access Law i.e., only that data that is already available through OBD ports.] See June 15 Tr. 125:19-22 (Smith) (“Q: And your dongle solution only works if mechanical

data is limited to what is already available through the OBD ports, correct? A: Yeah, that sounds right.”).

139. [Mr. Smith’s narrow reading of “mechanical data” is at odds with Section 1 of the Data Access Law, which defines “[m]echanical data” as data “otherwise related to the diagnosis, repair or maintenance of the vehicle,” including “telematics system data.” Data Access Law § 1 (codified at Mass. Gen. L. ch. 93K, § 1) (emphasis added). The inclusion of “otherwise related to” in the statutory definition necessarily means that the data at issue is broader than diagnosis, maintenance, and repair data themselves. Conclusion of Law ¶¶ 46-53; see also June 15 Tr. 24:3-6 (Lowe) (“Q: You agree with me that ‘otherwise related to’ was sort of a catch-all so that there would not be a narrow interpretation of what is related to diagnosis, repair and maintenance? A: Correct.”). Moreover, the inclusion of “telematics system data” in the statutory definition of “[m]echanical data” confirms that the data at issue exceeds that necessary for vehicle diagnosis, maintenance, or repair. Telematics data is not necessary to diagnose, maintain, or repair a vehicle. See Tierney Aff. ¶ 37; Baltes Aff. ¶ 30; Chernobly Aff. ¶ 43. As NHTSA explained, “[b]ecause all motor vehicle components potentially need maintenance, diagnostics, or repair at some point during their existence, this requirement effectively requires motor manufacturers to provide remote access to send commands to all of a vehicle’s systems – including braking, steering, and acceleration.” U.S. Statement of Interest (Dkt. 202) at 7.]

140. Even if Mr. Smith’s erroneous reading of mechanical data applied, his proposed “medium-term” solution utilizing a telematic-connected dongle does not exist and would expose vehicles to additional cybersecurity risk. Mr. Smith is not aware of any vendor who makes a dongle that an OEM could use to comply with the Data Access Law. June 15 Tr. 120:8-10 (Smith). Further, installing the dongle on the vehicle adds a new attack surface to the vehicle. June 15 Tr.

120:22-24 (Smith). A new attack surface means more risk to the vehicle's security. *See* June 15 Tr. 142:16-20 (Smith); June 16 Tr. 50:23-52:24 (Bort). Unlike a vehicle's telematics unit, the OBD-II port that the dongle would use to access the vehicle was not designed to accommodate a wireless connection and remain secure. June 16 Tr. 50:23-52:24 (Bort) ("the only thing we've done is provided a third party internet access to a vehicle in a way that the current design architecture was built to a physical access security model . . . The difference is that the telematics unit was designed into the defense in depth architecture to be interacted with in a certain way. A dongle going in through another point of access, no OEM would have built that."). Indeed, hackers and "security researchers," like Mr. Smith, have been able to use internet-connected dongles to hack into vehicles. June 15 Tr. 117:20-118:6, 142:4-15, 160:13-161:17 (Smith). Further, in addition to inherent risk of the dongle solution, OEMs must disable or reconfigure their secure gateways to allow the requisite access. June 15 Tr. 122:9-16 (Smith). Doing so would, at a minimum, "poke holes" in the gateway. June 15 Tr. 122:2-4 (Smith).

*Attempts to Comply with Section 3 Would Undermine Vehicle Safety and Emissions Integrity*

141. [An open access platform that facilitates a vehicle owner's and a third party's unfettered access to mechanical data presents significant security concerns, irrespective of the impossible timing demands of the Data Access Law.]

142. [For a platform to be open access, manufacturers could not be involved in the authentication and authorization process.] *See, e.g.,* Smith Aff. ¶ 115 ("to be 'open access' means to have a non-gated way to gain access to data and capabilities").

143. Section 3 thus requires that technicians and owners have the ability to write software to the vehicle for purposes of maintenance, diagnostics, and repair without the OEMs' approval. Data Access Law § 3; *see also* June 15 Tr. 82:23-83:12 (Lowe) (testifying that "write

commands and bi-directional capabilities” are “critical” to repairs); Smith Aff. ¶ 142 (“To fully support all mechanical diagnostics and repairs, independent repair shops and vehicle owners need to be able to perform three types of actions: (1) communicate through the gateway, (2) read and write diagnostic data to each ECU, and (3) transmit packets to the ECU.”).

144. [As discussed above, removing manufacturers from the process of authorizing the data written to the vehicle requires OEMs to disable cybersecurity controls and would substantially increase the risk of serious compromises to safety and emissions control.] See, e.g., June 14 Tr. 212:11-213:11 (Bort) (“open access would mean that the – you would only be able to have the holes in the Swiss cheese because anything else would be interpreted as the OEM being a part of the authorization to the vehicle. . . . so where I would go with this is that we’ve increased the risk aperture.”); June 15 Tr. 113:3-21 (Smith); June 15 Tr. 122:2-16 (Smith); Bort Aff. ¶¶ 59-60; June 14 Tr. 116:21-117:10 (Baltes); June 14 Tr. 71:22-3 (Tierney); June 14 Tr. 126:20-127:10 (Chernoby); Tierney Aff. ¶ 94; Chernoby Aff. ¶¶ 71, 73; Garrie Aff. ¶¶ 86-87. GM, for instance, would have to outright remove the following safety-critical cybersecurity controls (at a minimum): (i) gateways and firewalls that prevent unauthorized messages from reaching safety-related ECUs; (ii) access controls, including the challenge and response protocol as well as message authentication, (iii) firmware safeguards; and (iv) secured communication channels. See, e.g., Tierney Aff. ¶ 99; June 14 Tr. 116:13-17 (Baltes); June 14 Tr. 113:21-114:2 (Baltes); June 14 Tr. 115:2-7 (Baltes).

145. [Manufacturers would have to remove the secured gateway or, at the very least, undermine its functionality to comply with the Data Access Law’s broad data access requirements, including the ability of a mobile device to send commands to the ECUs.] See, e.g., June 15 Tr. 122:2-16 (Smith) (“Q: For your dongle solution, OEMs either need to remove any secured gateway

or poke holes in it; is that fair? A: Disable it or have holes, yes.”); June 14 Tr. 126:20-127:10 (Chernobyl) (“Q: Regardless of the time, though, you believe to create an open access platform, FCA would have to remove the secured gateway from the vehicle; is that correct? A: You would have to remove the functions that the gateway provides. You may be able to leave the piece of hardware there, but the type of authentication, et cetera, that it does would no longer be allowed.”).

146. Without the secured gateway and other authorization mechanisms, if a threat actor (or anyone else) gained access to the telematics system, nothing would prevent him or her from gaining access to safety-critical ECUs. *Id.*; *see also* Ex. 41 (AAI-GM-0001567); Bort Aff. ¶ 86; June 14 Tr. 114:19-115:1 (Baltes). Threat actors could develop and load custom code to a vehicle’s ECUs that could disable power steering, program emission control ECUs to be out of compliance with EPA emissions standards, or otherwise disrupt core vehicle functions related to safety and emissions. *See, e.g.*, June 14 Tr. 72:4-17 (Tierney); June 14 Tr. 89:2-90:4 (Tierney); June 14 Tr. 114:19-115:1 (Baltes).

147. [The Data Access Law’s mobile-based application requirement exacerbates cybersecurity threats while hamstringing manufacturers. Using secured communication protocols, manufacturers authenticate messages from current mobile applications before sending the message to the vehicle. Garrie Aff. ¶¶ 58-59; Tierney Aff. ¶¶ 73-74. The current configuration of these channels depends on the manufacturer managing and securing the communications with encryption keys held by the back office. Tierney Aff. ¶¶ 75, 77; Ex. 12 (AAI-GM-0001687). By vetting messages from the mobile application, manufacturers are able to identify malicious messages before they reach the vehicle. Garrie Aff. ¶¶ 37-38.] But the Data Access Law would prohibit this because the manufacturer would not be allowed to be involved in the authorization

process. June 15 Tr. 29:12-22 (Lowe) (explaining that the data must go directly from the vehicle to the owner's smartphone without first going through the manufacturer's servers).

148. [Removing manufacturers from the communication flow would immediately expose vehicles to significant risks from threat actors who gain access to a driver's phone.] See June 14 Tr. 118:20-22 (Baltes) ("We assume the [mobile] device is compromised, and if it's going to connect to the vehicle, we have to assert worst case."). [The lack of secure communication channels coupled with the Data Access Law's requirement that third parties be able to read and write new data to the vehicle is perilous because unauthorized third parties could take remote control of vehicles—taking command, for instance, of a vehicle's brakes or its steering wheel.] June 14 Tr. 118:14-18 (Baltes) ("the notion of having an additional wireless connection to not just an ECU but to the whole platform and networks is a little scary from a cyber perspective because it really broadens the attack service on the vehicle."); Garrie Aff. ¶¶ 90, 96-97; Tierney Aff. ¶ 104. [A threat actor would have the ability to write remotely malware to the vehicle via the telematics system, whereas now that ability either does not exist or is tightly controlled through key cybersecurity controls such as the secured gateway.] See Tierney Aff. ¶¶ 105-106 (explaining that, as part of its cybersecurity controls, GM does not permit its mobile application to write to the vehicle through the telematics system); Chernobly Aff. ¶ 82 (describing controls around over-the-air software updates that would be disabled to comply with the law); Smith Aff. ¶ 65.

149. [Further, the limited mobile data functionality some auto manufacturers currently allow is highly dissimilar from what the Data Access Law requires.] For example, GM's mobile application is limited to the transfer of some diagnostic codes and the deployment of a few customer-convenience commands, *e.g.*, remote start. Tierney Aff. ¶¶ 104-105. It does not reach safety-critical data or allow users to write new data to the vehicle. *Id.*; *see also* Garrie Aff. ¶ 93.

150. The GM mobile application has limited capabilities because of the controls in place to secure core vehicle functions. The mobile application is designed to communicate with the telematics system. Tierney Aff. ¶ 105. As previously described, the telematics system is purposefully isolated from safety and emissions related components. To allow a mobile application to send commands to these ECUs as required under the Data Access Law, the firewalls and central gateway module designed to support this isolation and secure these ECUs must be removed. *Id.*

151. [Finally, the requirement of standardization in Section 3 is also inconsistent with existing cybersecurity control protections utilized by OEMs.] Bort Aff. ¶¶ 64-65. For example, GM uses a “security-by-diversity” model that relies on using different systems on different products. Tierney Aff. ¶¶ 91-92. Having diverse systems means that infiltrating one system does not give threat actors a template to infiltrate an entire fleet of vehicles. *Id.*; Bort Aff. ¶ 65.

152. NHTSA has recognized this point as well. NHTSA’s 2016 Best Cybersecurity Practices guidance cautions that “[a]ny key obtained from a single vehicle’s computing platform should not provide access to multiple vehicles.” Ex. 3 at 17(NHTSA Cybersecurity Best Practices). [NHTSA repeated this point in its 2020 written testimony before the Massachusetts legislature about safety concerns with the Data Access Law. *See* Ex. 60 at 4 (NHTSA Testimony to Massachusetts Legislature).]

**E. NHTSA Has Confirmed that the Data Access Law Would Undermine Vehicle Cybersecurity and Risk a Recall**

153. [In NHTSA’s view, the Data Access Law would require manufacturers to “take actions that potentially pose serious cybersecurity risks by opening uncontrolled access to vehicle firmware that executes safety-critical functions, such as steering, acceleration, and braking, which are designed in a manner that expect (and require) authenticated privileged access rights in existing

implementations.” U.S. Statement of Interest (Dkt. 202) at 8; *see also* Ex. 60 at 5 (NHTSA Testimony to Massachusetts Legislature) (stating that the compliance requires OEMs to “redesign their vehicles in a manner that necessarily introduces cybersecurity risks, and to do so in a timeframe that makes design, proof, and implementation of any meaningful countermeasure effectively impossible.”).]

154. [More specifically, NHTSA made a “key recommendation” that “manufacturers should control access to firmware that executes vehicle functions,” adding that this is “particularly important for firmware controlling vehicle motion such as steering, acceleration, and braking.” U.S. Statement of Interest (Dkt. 202) at 4.] The Data Access Law’s requirement runs directly counter to NHTSA’s cybersecurity guidance. See Ex. 3 at 6.7.5 (NHTSA Cybersecurity Best Practices) (advising manufacturers that “signing techniques could prevent the installation of a damaging software update that did not originate from an authorized motor vehicle or equipment manufacturer”).

155. [NHTSA also noted that requiring standardized open access platform would create a substantial safety concern because it would not allow for the proper isolation of safety-critical functions. *See* U.S. Statement of Interest (Dkt. 202) at 8; Ex. 60 at 4 (NHTSA Testimony to Massachusetts Legislature); *see also* Ex. 60 at 4 (“[t]he ballot initiative would specifically require that vehicles be redesigned so that they are not isolated by mandating the ability to remotely ‘send commands to in-vehicle components’ such as steering, braking, and acceleration systems, thus creating another direct conflict with existing Federal guidance”).]

156. [The predictable effect of taking the actions required under the Data Access Law, NHTSA explained, would be to “create serious safety problems for motor vehicle owners,” by making it easier to hack into these vehicle functions and “cause a severe crash, potentially leading

to deaths or serious injuries.” U.S. Statement of Interest (Dkt. 202) at 6; *see also* Ex. 60 at 5 (NHTSA Testimony to Massachusetts Legislature).]

157. [Given the cybersecurity protections that manufacturers would have to disable, and NHTSA’s previous comments about cybersecurity, any attempt to comply with the Data Access Law would expose manufacturers to significant risk that NHTSA would order a recall because of the lack of protection for key vehicle safety features, particularly given that the Data Access Law does not provide any mechanism for safe compliance with the law’s requirements]

## **CONCLUSIONS OF LAW**

### **Jurisdiction and Venue**

1. The Court has jurisdiction over the subject matter of the litigation pursuant to 28 U.S.C. §§ 1331 and 2201(a) because the claims at issue at trial (counts I and II of the Complaint) arise under (a) the National Traffic and Motor Vehicle Safety Act (“Vehicle Safety Act”), 49 U.S.C. § 30101 *et seq.*; (b) the Clean Air Act, 42 U.S.C. § 7401 *et seq.*; and (c) the Supremacy Clause, U.S. Const. art. VI.

2. Venue is proper in this district pursuant to 28 U.S.C. § 1391(b) and (c).

### **Standing and Justiciability**

3. Auto Innovators has standing to bring this action on behalf of manufacturers. “An association has standing to sue on behalf of its members [if]: (1) at least one of the members possesses standing to sue in his or her own right; (2) the interests that the suit seeks to vindicate are pertinent to the objectives for which the organization was formed; and (3) neither the claim asserted nor the relief demanded necessitates the personal participation of affected individuals.”

*United States v. AVX Corp.*, 962 F.2d 108, 116 (1st Cir. 1992) (discussing *Hunt v. Wash. State Apple Advert. Comm.*, 432 U.S. 333, 343 (1977)).

4. It is undisputed between the parties that the first two factors for associational standing are met. Auto Innovators’ members, as manufacturers subject to the Data Access Law, have standing to sue in their own right to challenge that law. *See, e.g.*, Data Access Law §§ 2, 3 (codified at Mass. Gen. L. §§ 2(d)(1), (f)) (discussing new “manufacturer” obligations); Findings of Fact ¶¶ 2-3 (discussing vehicle sales in Massachusetts). And the interest that this suit seeks to vindicate is pertinent to the objectives for which Auto Innovators was formed. Findings of Fact ¶¶ 1, 4; *see also, e.g.*, <https://www.autosinnovate.org/about> (discussing Auto Innovators’ core

purpose to support cleaner, safer and smarter personal transportation that helps transform the U.S. economy, and sustain American ingenuity and freedom of movement).

5. The third prong of associational standing is a prudential prong. *United Food & Com. Workers Union Local 571 v. Brown Grp., Inc.*, 517 U.S. 544, 555-58 (1996).

6. The third prong of standing is also satisfied here. As the First Circuit has recognized, “just because a claim may require proof specific to individual members of an association does not mean the members are required to participate as parties in the lawsuit.” *Pharm. Care Mgmt. Ass’n v. Rowe*, 429 F.3d 294, 306 (1st Cir. 2005). This is particularly true when, as here, the remedy sought would “inure to the benefit” of all the association’s members. *Id.* at 307 (quoting *Warth v. Seldin*, 422 U.S. 490, 515 (1975)). Auto Innovators’ members are aligned in their inability to comply with both the Data Access Law and federal law as well as in their cybersecurity concerns about harm that would come from an attempt to implement the Data Access Law. *See, e.g.*, Findings of Fact ¶¶ 4-5, 5-16, 19-29, 33-37, 44-45, 52-63, 65-66, 73-80, 81-84, 91-95, 100, 102, 104-09, 111-14, 118-24, 126, 130; *see also Coll. of Dental Surgeons of Puerto Rico v. Conn. Gen. Life Ins. Co.*, 585 F.3d 33, 41 (1st Cir. 2009) (holding that there was associational standing even where adjudicating the claims “require[d] . . . evidence from individual” members, because the relief, if granted, would inure to the benefit of all members).

7. Importantly, all experts (for both parties) agreed that safe compliance with the Data Access Law is currently impossible for all manufacturers. *See* June 16 Tr. 41:21 (Smith); *id.* 42:1-5 (Romansky); *id.* 42:7-8 (Bort); *id.* 42:10 (Garrie).

8. Additionally, requiring manufacturers to standardize access to their systems would erase any diversity in approaches and leave each manufacturer vulnerable to cybersecurity attacks

in the same way. See June 14 Tr. 214:10-20 (Bort) (describing how “standardization” would lead to cybersecurity vulnerabilities applicable to all manufacturers).

9. The Attorney General’s own purported “solutions” undermine its claims that Auto Innovators lacks associational standing. The Attorney General’s experts have acknowledged that no solution currently exists to comply with the Data Access Law. See June 16 Tr. 41:21 (Smith); id. 42:1-5 (Romansky). That means that each manufacturer’s system would need to be modified.

10. Moreover, the Attorney General’s experts propose the same solutions for each manufacturer. None of the experts contends that some solutions would be appropriate for only some manufacturers. For example, the Attorney General’s experts all concede that the same third-party entity, utilizing the same standard for all manufacturers, would need to be used to fulfill the requirements of Sections 2 and 3. Findings of Fact ¶¶ 114-24; 131-34.

11. The type of relief that Auto Innovators seeks on behalf of its members provides further support for associational standing. Actions for “declaratory, injunctive and other forms of prospective relief have generally been held particularly suited to group representation.” *Students for Fair Admissions, Inc. v. President & Fellows of Harvard Coll.*, 261 F. Supp. 3d 99, 110 (D. Mass. 2017) (quoting *Camel Hair & Cashmere Inst. of Am. v. Associated Dry Goods Corp.*, 799 F.2d 6, 12 (1st Cir. 1986)), aff’d 980 F.3d 157 (1st Cir. 2020)).

12. In addition to associational standing, Auto Innovators has Article III standing to bring its pre-enforcement challenge because its individual manufacturer members have standing, and its claim is ripe for review.

13. A plaintiff has standing if he shows “(1) an ‘injury in fact,’ (2) a sufficient ‘causal connection between the injury and the conduct complained of,’ and (3) a ‘likel[ihood]’ that the

injury ‘will be redressed by a favorable decision.’” *Susan B. Anthony List v. Driehaus*, 573 U.S. 149, 157-58 (2014) (quoting *Lujan v. Defs. of Wildlife*, 504 U.S. 555, 560-61 (1992)).

14. As with other pre-enforcement challenges, the main concern is “the injury-in-fact requirement, there being no question that injury, if any, can be traced directly to the government’s threatened enforcement of the [statute] and can be redressed in this action.” *N.H. Lottery Comm’n v. Rosen*, 986 F.3d 38, 50 (1st Cir. 2021) (internal citations omitted). In a pre-enforcement challenge, the injury-in-fact requirement is met if the plaintiff alleges “an intention to engage in a course of conduct arguably affected with a constitutional interest, but proscribed by a statute, and there exists a credible threat of prosecution.” *Babbitt v. United Farm Workers Nat’l Union*, 442 U.S. 289, 298 (1979); see also *Susan B. Anthony List*, 573 U.S. at 161-65. This is not a high bar. See *N.H. Right to Life Pol. Action Comm. v. Gardner*, 99 F.3d 8, 14-15 (1st Cir. 1996) (collecting cases that found standing when “no criminal penalties had ever been levied under the statute,” *Babbitt*, 442 U.S. at 301, others where no plaintiff had been “threatened with prosecution,” *Doe v. Bolton*, 410 U.S. 179, 188 (1973), and finally one in which the Federal Election Commission “was split on the advisability of the [regulation] and there was no present danger of enforcement,” *Chamber of Com. v. Fed. Election Comm’n*, 69 F.3d 600, 603 (D.C. Cir. 1995)). These cases apply equally to commercial activity not affected with a First Amendment interest. See, e.g., *MedImmune, Inc. v. Genentech, Inc.*, 549 U.S. 118, 128-29 (2007) (allowing declaratory judgment action challenging patentability of invention underlying license agreement without requiring breach of that agreement); *Rosen*, 986 F.3d at 50-52 (allowing New Hampshire Lottery Commission to bring pre-enforcement challenge to the Wire Act to allow betting activity); *Alexis Bailly Vineyard, Inc. v. Harrington*, 931 F.3d 774, 778 (8th Cir. 2019) (business activity under the Commerce Clause is “arguably affected with a constitutional interest” for purposes of pre-

enforcement injury-in-fact). Manufacturers routinely manufacture vehicles for sale across state boundaries. See, e.g., Alexis Bailly Vineyard, Inc. v. Harrington, 931 F.3d 774, 778 (8th Cir. 2019) (business activity under the Commerce Clause is arguably affected with a constitutional interest).

15. The conduct at issue in this suit necessarily implicates the Supremacy Clause—immediately. Manufacturers are subject to stringent federal safety regulatory requirements. As the United States observed, manufacturers must certify compliance with federal vehicle safety standards, 49 U.S.C. § 30115; recall a vehicle if they determine that the vehicle contains a defect related to motor vehicle safety. *Id.* § 30116, 30118; report any defect to the Department of Transportation, notify affected owners, and provide owners with a free repair, refund, or replacement vehicle, *id.* §§ 30118-20; and remove any models subject to recall from the national market for new motor vehicles sales, *id.* § 30112(a). *See* U.S. Statement of Interest (Dkt. 202) at 2. Manufacturers have an immediate obligation to *self-initiate* a determination that a vehicle contains a safety-related defect, when the facts so support. *See id.* at 2-3; *accord United States v. Gen. Motors Corp.*, 574 F. Supp. 1047, 1049 (D.D.C. 1983) (Vehicle Safety Act imposes an “independent duty upon manufacturers of motor vehicles to give notification of and to remedy known safety defects,” whether or not NHTSA has opened a defect investigation or otherwise urged action on the part of the manufacturer). That statutory obligation to make timely determinations of safety defects and self-initiate recalls to remedy those defects applies to all motor vehicle manufacturers—at the risk of substantial civil penalties for failing to do so. *See, e.g.*, NHTSA Press Release, *NHTSA Announces Consent Order with Daimler Trucks North America* (Dec. 31, 2020), <https://www.nhtsa.gov/press-releases/nhtsa-announces-consent-order-daimler-trucks-north-america> (announcing a \$30 million civil penalty for untimely recalls).

16. As with the plaintiffs in *Virginia v. Am. Booksellers Ass'n, Inc.*, Auto Innovators has standing because “the law is aimed directly at plaintiffs, who, if their interpretation of the statute is correct, will have to take significant and costly compliance measures or risk [enforcement actions].” 484 U.S. 383, 392 (1988). There, as here, “[t]he State ha[d] not suggested that the newly enacted law will not be enforced.” *Id.* at 393. Just the opposite. The Attorney General has confirmed to this Court that it intends to enforce the law. The Data Access Law has already gone into effect, and the Attorney General has merely stayed enforcement *by its office*—which does not prevent a private right of action provided for under the statute, *see* Data Access Law § 5—for the limited time of this expedited trial. *See* Modified Stipulation at 1-2 (Dkt. 68) (“The 2020 Right to Repair Law will go into effect by December 18, 2020. . . . The Office of the Attorney General reserves the right to revise this stipulation in the event that adjudication of those claims is delayed beyond August 1, 2021, but further stipulates that it will do so only after first providing 14 days advance notice to Plaintiff and the Court of its intent to do so.”); *accord* June 25 Tr. 43:21-23 (Haskell) (“Our stipulation, Your Honor, was that—as I recall, we actually stipulated not to enforce it while this case is going on and reserve the right to revisit that.”).

17. Moreover, “[w]hen an individual is subject to . . . a threat, an actual . . . enforcement action is not a prerequisite to challenging the law.” *Susan B. Anthony List*, 573 U.S. at 158 (internal citation omitted). The Attorney General has done just that—clearing away any lingering doubt that she intends to enforce this law going forward. *See* June 25 Tr. 44:3-7 (“What I can say, Your Honor, and I can say this with confidence, is that what our office wants to see happen here is get to the right answer. And so if that means threatening enforcement to move things along, maybe that’s what it comes to.”).

18. And there is no debate from the Attorney General’s experts that the contested provisions of the Data Access Law cannot be met today. See Findings of Fact ¶¶ 5, 113-34. Nor can there be any debate that there is a causal connection between the injury to manufacturers and the complained-of conduct of. Cf. Susan B. Anthony List, 573 U.S. at 158. Whether to maintain existing cybersecurity protections (and thereby violate the Data Access Law) or attempt to comply with the open-access data regime mandated immediately by the Data Access Law (and thereby violate federal safety and emissions law) is a “direct and immediate dilemma” that manufacturers face. W.R. Grace & Co. v. EPA, 959 F.2d 360, 364 (1st Cir.1992). And a declaration stating that the Data Access Law is preempted, or enjoining the enforcement of that law, would redress that injury. Cf. Susan B. Anthony List, 573 U.S. at 158.

19. Ripeness in a pre-enforcement case is largely the same as the standing inquiry. See Rosen, 986 F.3d at 52 (internal citations omitted). Ripeness looks to both (a) “fitness,” *i.e.*, “finality, definiteness, and the extent to which resolution of the challenge depends upon facts that may not yet be sufficiently developed” and (b) hardship, *i.e.*, “whether the challenged action creates a direct and immediate dilemma for the parties.” *Id.* at 53 (internal citations and quotations omitted).

20. Generally, “a party’s ‘concrete plans to engage immediately (or nearly so) in an arguably proscribed activity’ gives a ‘precise shape to disobedience’ and provides a ‘specific legal question fit for judicial review,’ and a showing that a ‘challenged statute, fairly read, thwarts’ those plans can demonstrate hardship.” *Id.* (quoting *R.I. Ass’n of Realtors v. Whitehouse*, 199 F.3d 26, 33 (1st Cir. 1999)).

21. Manufacturers do not have to “expose [themselves] to liability before bringing suit to challenge the basis for a threat [of enforcement].” MedImmune, 549 U.S. at 129. The Attorney

General has already expressed its views on the Data Access Law, which it intends to enforce. The agency's "view having been expressed," "there ought to be a way to resolve the legal correctness of its position without subjecting" regulated entities to penalties as a precursor. *N.H. Hemp Council, Inc. v. Marshall*, 203 F.3d 1, 5 (1st Cir. 2000) (holding that a pre-enforcement statutory challenge is ripe, in part, because the threat of prosecution was "realistic," and observing that the discretionary nature of declaratory and injunctive relief counsels in favor of a flexible approach to justiciability).

22. The manufacturers have shown, and the Attorney General has not rebutted, that, as things stand today, manufacturers cannot comply with the Data Access Law. See Findings of Fact ¶¶ 5, 113-34. Because manufacturers cannot currently comply with the Data Access Law, they necessarily have concrete plans to engage in conduct prohibited by the statute. Auto Innovator's suit is therefore ripe for review. See, e.g., *Rosen*, 986 F.3d at 53 ("In the pre-enforcement context, a party's 'concrete plans to engage immediately (or nearly so) in an arguably proscribed activity' gives a 'precise shape to disobedience' and provides a 'specific legal question fit for judicial review,' and a showing that a 'challenged statute, fairly read, thwarts' those plans can demonstrate hardship.") (quoting *R.I. Ass'n of Relators*, 199 F.3d at 33).

#### **Plaintiff's Requested Relief Is Appropriate.**

23. Courts have long recognized a plaintiff's ability to seek injunctive relief against state officers' enforcement of unconstitutional state laws. See, e.g., *Ex parte Young*, 209 U.S. 123, 155-56 (1908). "It is beyond dispute that federal courts have jurisdiction over suits to enjoin state officials from interfering with federal rights." *Shaw v. Delta Air Lines, Inc.*, 463 U.S. 85 n.14 (1983); accord *Armstrong v. Exceptional Child Ctr., Inc.*, 575 U.S. 320, 326 (2015) ("If an

individual claims federal law immunizes him from state regulation, the court may issue an injunction upon finding the state regulatory actions preempted.”).

24. The cause of action in such cases comes not from any specific statutory or constitutional provision but from the court’s general equitable powers. *Armstrong*, 575 U.S. at 327; *Mich. Corr. Org. v. Michigan Dep’t. of Corr.*, 774 F.3d 895, 906 (6th Cir. 2014) (“Private parties who act in compliance with federal law may use *Ex parte Young* as a shield against the enforcement of contrary (and thus preempted) state laws. That makes sense, because an existing cause of action for that relief exists: an equitable anti-suit injunction.”) (internal citations omitted).  
*Armstrong* reaffirmed the viability of these claims, “subject to express and implied statutory limitations.” *Armstrong*, 575 U.S. at 327.

25. Contrary to the Attorney General’s assertion, see AG Conclusions of Law ¶ 15 (Dkt. 174), nothing in *Armstrong* suggested that a plaintiff must point to a federal statute giving the plaintiff a specific substantive federal right to vindicate.

26. Moreover, *Armstrong*, and lower courts interpreting *Armstrong* to require a private right of action, see, e.g., *Safe Streets Alliance v. Hickenlooper*, 859 F.3d 865, 902 (10th Cir. 2017), were cases in which plaintiffs sought an affirmative benefit. See *Armstrong*, 575 U.S. at 324 (seeking a more favorable Medicaid reimbursement rate); *Safe Streets Alliance*, 859 F.3d at 902-04 (requesting injunctive relief for enforcement of the Controlled Substances Act).

27. Auto Innovators does not seek to enforce a federal statute. Auto Innovators seeks only to be free from enforcement of an unconstitutional state law. This difference is fundamental. See *Mich. Corr. Org.*, 774 F.3d at 906 (contrasting “anti-suit injunctions” that have an “existing cause of action” with the situation in which “litigants wield *Ex parte Young* as a cause-of-action-creating sword” when “the State is not threatening to sue anyone”); see also *Armstrong v.*

Exceptional Child Center, Inc., 129 Harv. L. Rev. 211, 216 (2015) (interpreting *Armstrong* as preserving the distinction between affirmative and negative injunctions). Unsurprisingly, courts have found *Armstrong* to be no barrier to the type of preemption claim that Auto Innovators presents here. For example, in *Friends of the East Hampton Airport, Inc. v. Town of East Hampton*, the Second Circuit held that *Armstrong* did not foreclose plaintiffs' ability to sue to enjoin a municipal entity from enforcing "local laws enacted in violation of federal requirements," even though the federal statute vested enforcement authority in the Federal Aviation Administration and Secretary of Transportation, because the plaintiffs did not seek "to enforce the federal law themselves," 841 F.3d 133, 146 (2d Cir. 2016)—just as Auto Innovators does not seek to "enforce" the Vehicle Safety Act here, as evidenced by NHTSA's participation in this case. *Accord, e.g., United Healthcare of N.Y., Inc. v. Lacewell*, 967 F.3d 82, 90-91 (2d Cir. 2020); *Air Evac EMS, Inc. v. Texas, Dep't of Ins., Div. of Workers' Comp.*, 851 F.3d 507, 515-20 (5th Cir. 2017); *CNSP, Inc. v. Webber*, 2020 WL 2745456, at \*6 (D.N.M. May 27, 2020). Indeed, courts continue to address preemption claims in similar contexts. *Capron v. Off. of Atty. Gen. of Mass.*, 944 F.3d 9 (1st Cir. 2019); *Algonquin Gas Transmission, LLC v. Weymouth*, 919 F.3d 54 (1st Cir. 2019); *Cal. Trucking Ass'n v. Bonta*, 996 F.3d 644 (9th Cir. 2021); *Consumer Data Indus. Ass'n v. Frey*, 495 F. Supp. 3d 10 (D. Me. 2020).

28. Neither the Vehicle Safety Act nor the Clean Air Act evince an intention to limit the availability of equitable relief traditionally available under *Ex parte Young*. *Armstrong* relied on two aspects of the statutory scheme at issue to conclude that it foreclosed a cause of action: (1) that the statute provided only one mechanism as a remedy to hold states accountable for violating the statute; and (2) "the judicially unadministrable nature of [the statutory] text." *Armstrong*, 575

U.S. at 328. It was only the combination of these two characteristics that implied that Congress meant to foreclose the availability of equitable relief in Armstrong.

29. The Vehicle Safety Act does not provide an exclusive remedy. First, the Vehicle Safety Act specifies no particular enforcement mechanism against *states* for noncompliance. All of the Vehicle Safety Act's provisions relate to enforcement of the statute's requirements against vehicle manufacturers. Second, the remedies for enforcement under the Vehicle Safety Act are several. NHTSA can order a recall, 49 U.S.C. § 30118(b)(2), and fine manufacturers for failing to promptly notify consumers, 49 U.S.C. § 30121(b). If manufacturers do not comply, the federal government can sue manufacturers in federal court. 49 U.S.C. § 30163(a). And “[a]ny interested person may file a petition with the Secretary of Transportation requesting the Secretary to begin a proceeding . . . to decide whether to issue an order under section 30118(b).” 49 U.S.C. § 30162(a)(2).

30. Moreover, the Vehicle Safety Act imposes on manufacturers several affirmative duties. Manufacturers must “certify to the distributor or dealer . . . that the vehicle or equipment complies with applicable motor vehicle safety standards.” 49 U.S.C. § 30115(a). Manufacturers have obligations to “notify the Secretary [of Transportation]” of defects in a “vehicle or equipment” if the manufacturer “decides in good faith that the defect is related to motor vehicle safety,” 49 U.S.C. § 30118(c)(1), or “decides in good faith that the vehicle or equipment does not comply with an applicable motor vehicle safety standard,” 49 U.S.C. § 30118(c)(2). *See also* 49 U.S.C. § 30116(a) (imposing obligations on manufacturers for defects discovered before sales to customers). In practice, manufacturers take an active role in enforcement of the Vehicle Safety Act by working cooperatively with NHTSA to remove unsafe vehicles from the road. *See* U.S. Statement of Interest (Dkt. 202) at 2-3 (“Although DOT is authorized to issue recall orders, in

practice, the agency typically works with a motor vehicle manufacturer to comply with that manufacturer’s affirmative legal obligation to self-initiate a recall, rather than face the prospect of a recall order.”).

31. Nor is the Vehicle Safety Act judicially unadministrable. Cf. Armstrong, 575 U.S. at 328 (internal citations omitted) (finding Medicaid Act’s provision that payments be “consistent with efficiency, economy, and quality of care” while “safeguarding against unnecessary utilization of . . . care and services” judicially unadministrable). The Vehicle Safety Act explicitly contemplates that courts will have a role in deciding whether a safety issue is in fact a defect under the Vehicle Safety Act. 49 U.S.C. § 30163(a). Although such challenges are rare, they can hardly be said to be judicially unadministrable. Courts routinely determine whether the Vehicle Safety Act and FMVSS preempt state law. See, e.g., Williamson v. Mazda Motor of Am., Inc., 562 U.S. 323 (2011); Geier v. Am. Honda Motor Co., 529 U.S. 861 (2000); Hurley v. Motor Coach Indus., Inc., 222 F.3d 377, 382-83 (7th Cir. 2000); Griffith v. Gen. Motors Corp., 303 F.3d 1276 (11th Cir. 2002).

32. The same is true of the Clean Air Act. Although the Clean Air Act provides that an action to enforce its emissions standards “shall be brought by and in the name of the United States,” 42 U.S.C. § 7523(b), that does not necessarily mean that doing so is the only way that the standards can be enforced. And, like the Vehicle Safety Act, the EPA can force a recall of noncompliant vehicles. See 42 U.S.C. § 7541(c). And these provisions are far from judicially unadministrable, given that the United States can bring actions for the same violations. Indeed, courts routinely administer the Clean Air Act See, e.g., In re Volkswagen “Clean Diesel” Mktg., Sales Pracs., & Prods. Liab. Litig., 959 F.3d 1201 (9th Cir. 2020) (deciding whether the Clean Air Act preempted local regulations of pre- and post-sale vehicles); Minn. Auto. Dealers Ass’n v. Stine,

2016 WL 5660420, at \*8 (D. Minn. Sept. 29, 2016) (finding no foreclosure of equitable cause of action under similar provision of the Clean Air Act).

### **Burden of Proof**

33. “The burden to prove preemption rests with [the p]laintiff.” *Frey*, 495 F. Supp. 3d at 18 (citing *Capron*, 944 F.3d at 21).

34. There is no presumption against preemption for the claims that Auto Innovators asserts. The Supreme Court has held that preemption claims based on the Vehicle Safety Act are to be considered under “ordinary pre-emption principles,” without imposing any “special burden” on a preemption claim. *Geier*, 529 U.S. at 870; see also, e.g., *id.* at 888 (Stevens, J., dissenting) (taking issue with the majority’s “rejection” of a “presumption against pre-emption”). So, too, for preemption claims under the Clean Air Act and its implementing regulations. *In re Volkswagen “Clean Diesel” Mktg, Sales Practices, & Prods. Liab. Litig.*, 959 F.3d at 1213 (applying “ordinary pre-emption principles” to Clean Air Act preemption claim) (quoting *Geier*, 529 U.S. at 869, 874), *petition for cert. pending*, No. 20-994 (U.S.).

### **The 2013 Law**

35. Under Massachusetts law prior to enactment of the Data Access Law, auto manufacturers were already required to “provide access to their onboard diagnostic and repair information system[s]” and that, to the extent any proprietary device were necessary to access the data on those systems, to make that device “available to independent repair facilities upon fair and reasonable terms.” Mass. Gen. L. ch. 93K, § 2(d)(1) (the 2013 so-called “Right to Repair Law”).

36. Specifically, the 2013 Law required auto manufacturers “to provide independent repair shops with the same data that's necessary for diagnosis, maintenance and repair that was provided to dealers.” June 15 Tr. 15:17-20 (Lowe); *see* Mass. Gen. Laws ch. 93K, § 2(d)(1) (2013

Right to Repair Law); Potter Aff. ¶ 20; Tierney Aff. ¶ 78. That law also provided specific, detailed standards to govern the standardized access, see Mass. Gen. L. ch. 93K, § 2(d)(1) (discussing SAE J2534, SAE J1939, and ISO 22900)—which stands in stark contrast to the Data Access Law, see, e.g., June 15 Tr. 94:5-95:11 (Potter) (stating that he was surprised that requirements as complex as the Data Access Law’s were not given more clarity than a four-page bill).

37. Thus, prior to the Data Access Law, Chapter 93K required that auto manufacturers provide access to on-board diagnostic (“OBD”) systems. *See* Mass. Gen. Laws ch. 93K, § 2(d)(1) (“Each manufacturer shall provide access to the same onboard diagnostic and repair information available to their dealers, including technical updates to such onboard systems....”); *see also* Findings of Fact ¶¶ 99-100; June 15 Tr. 82:23-83:12 (Lowe); June 16 Tr. 93:17-94:5 (Garrie) (under existing law, “independent repair technicians need to have the same ability to repair motor vehicles as dealers,” and “that includes the ability to modify the software on the vehicle”); Smith Aff. ¶ 53 (“Advanced diagnostic tools can write and modify data in order to fix or correct a problem with the vehicle.”).

38. The access provided under the 2013 Law encompasses the ability to write to and modify the software on an ECU. Findings of Fact ¶ 14; AG’s Proposed Findings of Fact ¶ 105 (Dkt. 174) (In GM vehicles, “a small number of ‘programming’ diagnostic functions support reprogramming of other software updates to ECUs.”); Ex. 527 at 2 (AAI-ACA-0000226) (noting that certain types of reprogramming subscriptions are required by the 2013 Law and the MOU); Potter Aff. ¶ 24 (noting that dealership tools “perform some reprogramming and reconfiguring functions.”); June 15 Tr. 82:23-83:12 (Lowe) (testifying that “write commands and bi-directional capabilities” are “critical” to repairs and explaining that technicians frequently have to download the “latest software updates” to a vehicle to complete the repair).

39. Aftermarket groups represented by, among others, the Auto Care Association, entered into a Memorandum of Understanding (MOU) with the predecessor organization to Auto Innovators and auto manufacturers that auto manufacturers would comply voluntarily nationwide with the provisions of the 2013 Law. Ex. 1 (AAI-AAI-0002635); June 15 Tr. 15:25-16:12 (Lowe). And although the MOU provides for a dispute resolution process, manufacturers and the aftermarket have always worked through any compliance issues without a formal decision through the MOU's dispute resolution process. June 15 Tr. 60:18-25 (Lowe).

### **The Data Access Law**

40. The Data Access Law goes well beyond the requirements of the 2013 Law through a series of amendments, revisions, and additions to Chapter 93K of the Massachusetts General Laws. *See generally* Data Access Law (codified at Mass. Gen. L. ch. 93K, §§ 1, 2(d)(1), 2(f)-(h), 6).

41. The Attorney General argues that, as the agency responsible for enforcement of the Data Access Law, her office is entitled to deference in its interpretation of several of the terms that the Data Access Law added to Chapter 93k. Although an enforcing agency is typically entitled to some deference, no deference is required to interpretations that are contrary to “the plain language of the statutory provisions.” *Smith v. Winter Place LLC*, 447 Mass. 363, 368 (2006); *see also Leopoldstadt, Inc. v. Comm'r of Div. of Health Care Fin. and Pol'y*, 436 Mass. 80, 91 (2002) (“[T]his principle is one of deference, not abdication, and we have overruled an agency’s interpretation when it is contrary to the plain language of the statute and its underlying purpose.”) (internal quotations and citations omitted). As the Supreme Judicial Court has recognized, the issue of deference should not even be considered unless the statute or regulation at issue is “genuinely ambiguous.” *DeCosmo v. Blue Tarp Redevelopment, LLC*, 487 Mass. 690, 700 (2021).

42. And any deference is particularly limited when the agency's interpretation is "developed during, or shortly before, the litigation in question," *Mullally v. Waste Mgt. of Mass., Inc.*, 452 Mass. 526, 533 n.13; see also *DeCosmo*, 487 Mass. at 702-03, and is in an area in which the agency has no technical or "special competence" to determine a term's meaning, *Souza v. Registrar of Motor Vehicles*, 462 Mass. 227, 229 (Mass. 2012); accord *DeCosmo*, 487 Mass. at 699, 702 (discussing the "substantive expertise" requirement).

43. The Attorney General's interpretations do not warrant any deference; as explained below, those interpretations attempt to define unambiguous language or conflict with the plain meaning of the Data Access Law. See, e.g., *Pub. Empl. Ret. Sys. of Ohio v. Betts*, 492 U.S. 158, 171 (1989) ("[N]o deference is due to agency interpretations at odds with the plain language of the statute itself."). The Office of the Attorney General had no role in crafting the language ballot initiative, has no experiencing enforcing the law arising from the ballot initiative or its predecessor, and has not engaged in (and is not called to engage in) any agency rulemaking. Indeed, the Data Access Law's requirements are self-executing. The requirements in Section 2 of the Act took effect one month after the law's passage and apply retroactively to model year 2018 vehicles. See Mass. Const. amends. art. 48, pt. V, § 1; Data Access Law § 2 (codified at Mass. Gen. Laws ch. 93K, § 2(d)(1) (2020)). The requirements in Section 3 also have already taken effect, but apply to model year 2022 vehicles and newer. See Mass. Const. amends. art. 48, pt. V, § 1; Data Access Law § 3 (codified at Mass. Gen. Laws ch. 93K, § 2(f) (2020)). Neither section depends on whether and when the Attorney General will eventually comply with her separate, limited obligation under Section 4 to craft a notice about telematics systems and data that dealers would then have to provide to prospective owners. See Data Access Law §§ 2-4.

44. Nor does the Office of the Attorney General have any special competence in the area of automobile safety and cybersecurity. When, as here, an agency offers an interpretation on statutory terms “unrelated” to the agency’s “specialized knowledge” and for which it has no “special competence to determine what the Legislature [or voters] meant,” “the interpretive question . . . is purely a legal one” and the agency’s interpretation is reviewed de novo. *Souza*, 462 Mass. at 229-30. NHTSA, on the other hand, has decades of expertise in matters of vehicle safety. *See, e.g., Motor Vehicle Mfrs. Ass’n of U.S., Inc. v. State Farm Mut. Auto. Ins. Co.*, 463 U.S. 29, 53 (1983) (noting that what conclusion to be drawn from studies regarding seat belt usage was “precisely the type of issue . . . within the expertise of NHTSA, and upon which a reviewing court must be most hesitant to intrude.”); *Nat’l Truck Equip. Ass’n v. Nat’l Highway Traffic Safety Admin.*, 711 F.3d 662, 672 (6th Cir. 2013) (deferring to NHTSA’s determination about whether a particular process would increase manufacturers’ compliance costs because such a determination was in NHTSA’s scope of expertise); *see also* U.S. Statement of Interest (Dkt. 202) at 2 n.3 (noting that NHTSA has authority to enforce the Vehicle Safety Act).

#### A. New Definitions

45. Section 1 of the Data Access Law adds a new definition—“[m]echanical data”—that it defines to include “any vehicle-specific data, including telematics system data, generated, stored in or transmitted by a motor vehicle used for or otherwise related to the diagnosis, repair or maintenance of the vehicle.” Data Access Law § 1 (codified at Mass. Gen. L. ch. 93K, § 1).

46. “Mechanical data” includes some subset of vehicle “telematics” data (Data Access Law § 1 (codified at Mass. Gen. L. ch. 93K, § 1)) because that data is referenced directly in the law. *See, e.g., Friends of the Earth, Inc. v. EPA*, 446 F.3d 140, 145 (D.C. Cir. 2006) (when words are used in the law itself, that “settle[s] the question” of the law’s reach).

47. “Mechanical data” also includes data beyond that necessary for vehicle diagnosis, repair, or maintenance by applying to data “otherwise related to the diagnosis, repair or maintenance of the vehicle.” Data Access Law § 1 (codified at Mass. Gen. L. ch. 93K, § 1) (emphasis added). Courts confronted with the terminology “otherwise related to” in other contexts have observed that the effect is to create a “broadly worded” obligation that extends beyond the terms modified by that language. See, e.g., *Khan v. Parsons Global Servs., Ltd.*, 521 F.3d 421, 423 (D.C. Cir. 2008) (discussing an “otherwise related to” arbitration clause). The plain language of the definition of “[m]echanical data” is directed at data other than merely diagnosis data, repair data, or maintenance data, and must be read as such. See, e.g., *In re Rudler*, 576 F.3d 37, 44 (1st Cir. 2009) (“If the statute’s language is plain, the sole function of the courts—at least where the disposition required by the text is not absurd—is to enforce it according to its terms.”) (internal quotations omitted).

48. The Attorney General suggests a narrow reading of “mechanical data,” interpreting the term to include only repair data accessible through a vehicle’s OBD ports and telematics. E.g., AG Conclusions of Law ¶¶ 36-38. This interpretation does not comport with the plain language of the statute.

49. The statute defines “[m]echanical data” to include “any vehicle-specific data, including telematics system data, generated, stored in or transmitted by a motor vehicle used for or otherwise related to the diagnosis, repair or maintenance of the vehicle.” Data Access Law § 1 (emphasis added). By its plain terms, that data is broader than that merely “used” for diagnosis, repair, or maintenance. It is longstanding Massachusetts law that “none of the words of a statute is to be regarded as superfluous, but each is to be given its ordinary meaning.” *Commonwealth v.*

Woods Hole, Martha's Vineyard and Nantucket S.S. Auth., 352 Mass. 617, 618 (1967) (internal quotations and alterations omitted).

50. Moreover, proponents of the Data Access Law intended the term “mechanical data” to have a broader meaning than that proposed by the Attorney General. Mr. Lowe—who helped draft the ballot initiative and whose organization was heavily involved in the initiative process, see June 15 Tr. 13:5-12—confirmed that the “otherwise related to” language was intended as a “catch-all” to ensure the term “mechanical data” would not be interpreted narrowly. *Id.* 24:3-6.

51. The Attorney General’s limited reading of the term “mechanical data” would also render Section 2 of the Data Access Law superfluous to other, preexisting provisions of Chapter 93K. The preexisting provisions of Chapter 93K required OEMs to provide access to all data necessary for diagnosis, repair, and maintenance. *See* Mass. Gen. Laws ch. 93K, § 2(d)(1) (2013 Right to Repair Law); Potter Aff. ¶¶ 10-11; Tierney Aff. ¶ 78. By its plain terms, Section 2 of the Data Access Law expands the scope of Chapter 93K to a larger universe of vehicle data, which includes, but is not limited to, the “mechanical data” strictly necessary for diagnosis, repair, and maintenance.

52. And as the United States explained, expressing the view of NHTSA—the agency with decades of technical expertise in vehicle safety—“[b]ecause all motor vehicle components potentially need maintenance, diagnostics, or repair at some point during their existence, [the] requirement [to provide access to “mechanical data”] effectively requires motor vehicle manufacturers to provide remote access to send commands to all of a vehicle’s systems—including braking, steering, and acceleration.” Dkt. 202 at 7.

53. Considering the language of the Data Access Law and the United States’ reasonable opinions on its scope, “mechanical data” cannot be read as narrowly as the Attorney General

proposes. Rather, the term encompasses all or some portion of the data generated by and related to safety-critical systems and emissions-control systems regulated by NHTSA and the EPA.

54. Section 1 of the Data Access Law also introduces another definition to Massachusetts law—“[t]elematics system”—which it defines as “any system in a motor vehicle that collects information generated by the operation of the vehicle and transmits such information, in this chapter referred to as ‘telematics system data,’ utilizing wireless communications to a remote receiving point where it is stored.” Data Access Law § 1 (codified at Mass. Gen. L. ch. 93K, § 1).

**B. New Substantive Requirements—Section 2**

55. Section 2 of the Data Access Law amends existing Massachusetts law to remove manufacturers’ ability to control who is authorized to access their vehicle systems. It mandates that “on-board diagnostic systems”—a term it does not define—“shall be standardized and not require any authorization by the manufacturer, directly or indirectly, unless the authorization system for access to vehicle networks and their on-board diagnostic systems is standardized across all makes and models sold in the Commonwealth and is administered by an entity unaffiliated with a manufacturer.” Data Access Law § 2 (codified at Mass. Gen. L. ch. 93K, § 2(d)(1)).

56. By proscribing “any authorization by the manufacturer, directly or indirectly,” Section 2 of the Data Access Law eliminates manufacturers from the process of authorizing access to vehicle diagnostic systems. Data Access Law § 2 (codified at Mass. Gen. L. ch. 93K, § 2(d)(1)) (emphasis added). The phrase “directly or indirectly” is yet another signal of a “broad” prohibition. *Burley v. Comets Cnty Youth Ctr., Inc.*, 75 Mass. App. Ct. 818, 821 (2009) (quoting *N. Am. Expositions Co. Ltd. P’ship v. Corcoran*, 452 Mass. 852, 862 (2009)); accord *Manning v. Zuckerman*, 388 Mass. 8, 14 (1983) (describing “directly or indirectly” as “broad language”) (internal quotations omitted).

57. “Authorization,” at a minimum, encompasses “an actor’s role, or what the actor is and is not permitted to do on a system.” Attorney General’s Post-Evidence Memorandum at 3 (Dkt. 217). Compliance with Section 2 requires removing any form of authorization that an auto manufacturer has in place on its vehicles unless such authorization is administered by an independent third party entity. June 15 Tr. 125:15-18 (Smith). No such third party entity exists at the present time. Findings of Fact ¶ 114.

58. As the Attorney General’s expert witnesses concede, Section 2 requires removing at least some types of authorization, including ECU authentication, message authentication, and secure gateways. June 15 Tr. 125:15-18 (Smith); Smith Aff. ¶ 141; *see also* Tierney Aff. ¶ 51-56 (describing message authentication); Chernobyl Aff. ¶ 67 (“For example, FCA would have to remove challenge and response protocols and message authentication because both require the manufacturer to be involved in the authorization process.”); June 14 Tr. 229:14-22 (Bort) (absence of authorization requirement requires removal of secure gateway). These authorization mechanisms relate directly to vehicles’ safety-critical functions, including by preventing hackers from accessing vehicles’ diagnostic functions. *See* Smith Aff. ¶ 144 (By employing ECU authorization, “attackers are prevented from accessing [] diagnostic functions without the requisite authorization); *id.* ¶ 154-55 (“the goal of message authentication is to prevent an attacker from replaying or spoofing (faking) packets on a network.”); June 15 Tr. 121:24-122:1 (“gateways help keep vehicles safe from a cybersecurity standpoint.”).

59. The Attorney General urges that Section 2 does not require removal of these cybersecurity features because these features relate to “authentication” and not “authorization.” That directly contradicts the Attorney General’s experts’ opinions. *See, e.g.*, Smith Aff. ¶ 144 (“Since each ECU checks the level of access before allowing write access, attackers are prevented

from accessing these diagnostic functions without the requisite authorization"); *id.* ¶ 146 (diagnostics "that do not require authorization" are at the security level of "anonymous access," but that OEMs impose authorization requirements on other access to diagnostic functionality); *id.* ¶ 164 ("Currently, some OEMs employ a secure gateway to manage authorization of third-party tools and mechanics."); June 15 Tr. 125:15-18 (Smith) ("Q: And if the OEMs can't transfer authorization access to this third party, they would have to disable ECU or message authentication, wouldn't they? A: That's correct."); Romansky Aff. ¶ 20 ("[A]uthentication and authorization are terms used to describe the process of validating the identity and authentic access rights of a remote user or system. For example, when a repair technician uses a scan tool to read or write to an ECU within a vehicle, the vehicle network can optionally require that the technician or the scan tool prove that they have the correct access rights to interact with the vehicle").

60. Regardless, the Attorney General's arguments regarding "authentication" versus "authorization" make a distinction without a difference. Nothing in the statute excludes "authentication" and, as these concepts are understood within the industry, "authentication is necessarily intertwined with the concept of "authentication." Romansky Aff. ¶ 20 ("authentication and authorization are terms used to describe the process of validating the identity and authentic access rights of a remote user or system"); June 14 Tr. 210:24-211:3 (Bort) (authorization and authentication "only work together"); June 14 Tr. 249:15-19 (Garrie) (authentication and authorization "are interchangeable" and one is "ineffective" without the other).

61. Reliance upon the industry understanding of these terms is particularly apt "when interpreting a statute about computers." *Van Buren v. United States*, 141 S. Ct. 1648, 1657 (2021). Indeed, the Supreme Court recently described authentication as "a specific type of authorization"

that “turns on whether a user’s credentials allow him to proceed past a computer’s access gate, rather than on other scope-based restrictions.” *Id.* at 1659 n.9 (internal quotations omitted).

62. The term “authorization” cannot reasonably be interpreted so narrowly as to exclude “authentication.”

63. Section 2 contemplates, as an alternative to abandoning manufacturer authorization outright, an independently administered “authorization system for access to vehicle networks and their on-board diagnostic systems” that is “standardized across all makes and models sold in the Commonwealth.” Data Access Law § 2 (codified at Mass. Gen. L. ch. 93K, § 2(d)(1)) (emphasis added). The plain language of the statutory provision thus encompasses not only “on-board diagnostic systems” but also “vehicle networks” of which on-board diagnostic systems are only a part. *Id.*

64. Section 2 of the Data Access Law also imposes a uniform standardization requirement for access to certain vehicle systems. Data Access Law § 2 (codified at Mass. Gen. L. ch. 93K, § 2(d)(1)) (requiring either that “on-board diagnostic systems shall be standardized and not require any authorization by the manufacturer, directly or indirectly” or the “authorization system for access to vehicle networks and their on-board diagnostic systems is standardized across all makes and models sold in the Commonwealth”).

65. The term “standardized across all makes and models sold in the Commonwealth” encompasses vehicles manufactured by all manufacturers, not just those within each manufacturer. Ex. 30 at 3 (Def.’s 2d Suppl. Resps. to Pl.’s 1st Set of Interrogatories (Apr. 30, 2021)). The Data Access Law is silent, however, on how such standardization across manufacturers (*i.e.* all makes and models in the entire motor vehicle industry) is to be achieved, as the Data Access Law neither references any such uniform standards nor establishes any process for such standards to be created.

*See generally* Data Access Law. As the evidence presented at trial shows, the standardized authorization system required by Section 2 does not exist at the present time. Findings of Fact ¶ 114.

66. Section 2 also requires the authorization system to be administered “by an entity unaffiliated with a manufacturer.” Data Access Law § 2 (codified at Mass. Gen. L. ch. 93K, § 2(d)(1)). This is not limited to entities with no corporate affiliation with a manufacturer, but also applies to entities over which an auto manufacturer exercises direct or indirect control. Ex. 30 at 3 (Def.’s 2d Suppl. Resps. to Pl.’s 1st Set of Interrogatories (Apr. 30, 2021)). No such entity exists at this time. Findings of Fact ¶ 114.

67. “[V]ehicle networks” is not defined in the Data Access Law itself or in Chapter 93K. *See generally* Mass. Gen. L. ch. 93K. The term does not mean simply “on-board diagnostic systems,” because it is referred to in the statute independently of those systems. To conflate the two would run afoul of the rule to “avoid interpretations that render statutory language mere surplusage.” *Maine Pooled Disability Tr. v. Hamilton*, 927 F.3d 52, 58 (1st Cir. 2019) (quoting *Lawless v. Steward Health Care Sys., LLC*, 894 F.3d 9, 23 (1st Cir. 2018)); *Flemings v. Contributory Retirement Appeal Bd.*, 431 Mass. 374, 375 (2000) (“In interpreting statutes, none of the words of a statute is to be regarded as superfluous, but each is to be given its ordinary meaning without overemphasizing its effect upon the other terms appearing in the statute . . . .”) (internal quotations and brackets omitted).

68. The Attorney General interprets the term “vehicle networks” to be synonymous with OBD systems. AG Tr. Mem. 14 (Dkt. 172); AG Conclusions of Law ¶ 80; see also June 15 Tr. 124:5-12 (Smith) (reading “vehicle networks” no broader than a vehicle’s OBD system); *id.* 188:22-189:6 (Romansky) (opining only on OBD systems for Section 2).

69. But as the Attorney General’s own experts note, however, vehicle networks and on-board diagnostic systems are different things that serve different roles in a vehicle. June 15 Tr. 187:8-22 (Romansky). A vehicle network is a communication network within a vehicle, and any given vehicle might have multiple vehicle networks separate by gateways or firewalls. *Id.* 186:9-187:1 (Romansky). The Statement of Interest of the United States supports reading “vehicle networks” to include systems such as the “vehicle firmware that executes safety-critical functions, such as steering, acceleration, and braking.” U.S. Statement of Interest (Dkt. 202) at 8.

70. In addition, the Data Access Law uses the terms “vehicle networks” and “on-board diagnostic systems” independently. Interpreting them to be synonymous, as the Attorney General urges, would contravene established principles of statutory interpretation not to give two different terms the same meaning. *See, e.g., Tamulevich v. Robie*, 426 Mass. 712, 714 (1998) (declining to construe two different terms in a statute as synonymous because, by including both, “the Legislature would not likely have used them to mean the same thing”).

71. Thus, based on the industry understanding advanced by the Attorney General’s own experts, the implied definition utilized by the United States, and the language of the Data Access Law, the term “vehicle networks” is not limited to OBD systems and encompasses a broader range of vehicle systems which may include networks governing safety-critical functions, such as steering, acceleration, and braking.

72. The requirements in Section 2 of the Data Access Law apply retroactively to model year 2018 vehicles. *See* Mass. Gen. L. ch. 93K, § 2(d)(1).

73. The requirements in Section 2 of the Data Access Law became effective in December 2020. *See* Mass. Const. amends. art. 48, pt. V, § 1; *see also* Mass. Gen. L. ch. 54, § 112 (describing election-result certification process). Despite the Data Access Law’s effective date,

the parties agree that no means for compliance with Section 2 currently exists. Findings of Fact ¶¶ 104, 113-15; Ex. 27 at 3 (Def.’s 2d Suppl. Resps. to Pl.’s 1st Set of Requests for Admission (April 30, 2021)) (“[T]he Attorney General further states that she is not aware of any existing ‘authorization system for access to vehicle networks and their on-board diagnostic systems’ that is ‘standardized across all makes and models sold in the Commonwealth and is administered by an entity unaffiliated with a manufacturer.’”). The Attorney General’s experts agreed. Findings of Fact ¶ 114; *see also* June 15 Tr. 193:21-197:13 (Romansky); June 15 Tr. 118:11-13, 125:6-9 (Smith).

### **C. New Substantive Requirements—Section 3**

74. Section 3 of the Data Access Law requires each manufacturer that “utilizes a telematics system” in any of its vehicles to equip any vehicle sold in Massachusetts with a novel “open access” vehicle telematics platform. Data Access Law § 3 (codified at Mass. Gen. L. ch. 93K, § 2(f)). Vehicles using those systems must be equipped with “an inter-operable, standardized and open access platform across all . . . makes and models” “[c]ommencing in model year 2022.”

*Id.*

75. An “open access platform” is not defined in the Data Access Law. As commonly understood in the technical field, “open access” denotes without restriction. *In re Carrier IQ, Inc.*, 78 F. Supp. 3d 1051, 1100-01 (N.D. Cal. 2015) (quoting *Opperman v. Path, Inc.*, No. C13-0453-JST, 2014 WL 1973378, at \*21 (N.D. Cal. May 14, 2014)). The Attorney General interprets the term “open access” to allow the use of “security controls to ensure the safety and privacy of the consumer.” Attorney General’s Post-Evidence Memorandum 6 (Dkt. 217). Nothing in the term “open access” suggests such a limitation. See, e.g., U.S. Statement of Interest (Dkt. 202) at 7 (“Importantly, . . . open access must ‘include the ability to send commands to in-vehicle

components if needed for purposes of maintenance, diagnostics, and repair.’ Because all motor vehicle components potentially need maintenance, diagnostics, or repair at some point during their existence, this requirement effectively requires motor vehicle manufacturers to provide remote access to send commands to all of a vehicle’s systems—including braking, steering, and acceleration.”) (quoting Data Access Law § 3); *id.* at 8 (“[T]he Data [Access] Law effectively requires open remote access, potentially accessible by anyone, to all of a motor vehicle’s telematics systems.”); *see also id.* at 6 (describing the 2015 FCA cybersecurity recall as necessary “in order to close the open access”).

76. Under Section 3, the “inter-operable, standardized and open access platform” required must be “directly accessible” by the vehicle owner through an (undefined) “mobile-based application” as well as by independent repair facilities. Data Access Law § 3 (codified at Mass. Gen. L. ch. 93K, § 2(f)). A “mobile-based application” means an application on a mobile phone. See June 15 Tr. 29:12-22 (Lowe) (explaining that the data must go directly from the vehicle to the owner’s smartphone without first going through the manufacturer’s servers); Ex. 509 at 4 (“Owners of motor vehicles with telematics systems would get access to mechanical data through a mobile device application.”). In order for a platform to be “inter-operable” it must utilize “a standard way to connect and communicate with the vehicle.” An inter-operable “device is one that can be used regardless of the manufacturer. Attorney General’s Post-Evidence Mem. 6 (Dkt. 217).

77. “Standardized” means “a common and well documented method to perform the necessary actions such that there is a common, agreed upon way of communicating.” Attorney General’s Post-Evidence Mem. 6 (Dkt. 217).The platform must also allow those parties “to send commands to in-vehicle components if needed for purposes of maintenance, diagnostics and repair.” Data Access Law § 3 (codified at Mass. Gen. L. ch. 93K, § 2(f)).

78. Further, the platform must be “capable of securely communicating all mechanical data emanating directly from the motor vehicle via direct data connection to the platform,” Data Access Law § 3 (codified at Mass. Gen. L. ch. 93K, § 2(f))—with “[m]echanical data” defined separately, as discussed above, to include any data “otherwise related to the diagnosis, repair or maintenance of the vehicle,” including “telematics data,” *id.* § 1 (codified at Mass. Gen. L. ch. 93K, § 1).

79. At the present time neither the mobile-based application nor the secure platform for transmission of data directly from the vehicle, as required by Section 3, exist. Findings of Fact ¶ 123.

80. The Data Access Law’s reference to “a manufacturer of motor vehicles sold in the Commonwealth” (Data Access Law § 3 (codified at Mass. Gen. L. ch. 93K, § 2(f))) requires a nexus between the manufacturer and the sale in the Commonwealth. A reading of the law that would unconstitutionally impose on manufacturers regulatory obligations (and penalties) for vehicles later sold by third parties in the Commonwealth would explicitly require them to follow Massachusetts law for vehicles they sell, through dealerships, in other states. To avoid that glaring constitutional infirmity, the Data Access Law must be read to apply only to an initial sale of a vehicle from a manufacturer or its affiliated dealers to a consumer. See, e.g., Commonwealth v. Gustafsson, 370 Mass. 181, 190 (1976) (“It is well settled that a statute must be read so as to avoid constitutional doubts.”).

81. Despite the requirements in Section 3 “[c]ommencing in model year 2022,” Data Access Law § 3 (codified at Mass. Gen. L. ch. 93K, § 2(f)), the parties agree that no means for compliance with Section 3 currently exist. Findings of Fact ¶¶ 104, 122-24; Ex. 27 at 5 (Def.’s 2d Suppl. Resps. to Pl.’s 1st Set of Requests for Admission (April 30, 2021)) (“[T]he Attorney

General further states that . . . she is not aware of any platforms that meet the requirements of Section 3 of the 2020 Right to Repair Law that are currently commercially available . . .”)

82. When asked by this Court whether OEMs could provide the inter-operable, standardized, open access platform required by the Data Access Law, every expert agreed that they could not. *See* June 16 Tr. 41:21 (Smith) (“Definitely not right away.”); *id.* 42:1-3 (Romansky) (“I think the elements of a solution are available, but they’re not assembled, and that has not been proven to all work together.”); June 15 Tr. 198:23-24 (Romansky) (“I’m not aware of any [telematics systems] that fully comply with Section 3, correct.”); June 16 Tr. 42:7-8 (Bort) (“I don’t think we can do that right now.”); *id.* 42:10 (Garrie) (“I agree with my colleagues.”). Aside from the platform itself, there is also no “mobile-based application” (Data Access Law § 3) to comply with the law. E.g., June 15 Tr. 95:21-96:17 (Potter); *id.* 126:13-15 (Smith).

83. [Even aside from federal preemption issues, it is unconstitutional to subject manufacturers to stiff penalties for violating a law with which they cannot comply. A law that commands someone to perform an impossible act is unconstitutional under the Due Process Clause. E.g., *United States v. Dexter*, 165 F.3d 1120, 1125 (7th Cir. 1999).]

84. Though an automaker may in theory be able to avoid falling under the scope of Section 3 of the Data Access Law by disabling the telematics systems of vehicles sold in the Commonwealth, doing so would not resolve the preemption issues created by Section 3. By its plain terms, Section 3 requires manufacturers to deploy “an inter-operable, standardized and open access platform across all . . . makes and models” “[c]ommencing in model year 2022.” Data Access Law § 3 (codified at Mass. Gen. L. ch. 93K, § 2(f)). And Section 3 then applies that requirement to “a manufacturer of motor vehicles sold in the Commonwealth . . . that utilizes a telematics system.” *Id.* Manufacturers that utilize a telematics system thus constitute the regulated

entities under the Data Access Law. It is well-established that, in assessing whether state law requirements are preempted, a regulated entity's ability to avoid the state law's requirements by ceasing the business operations that make it a regulated entity under that law in the first place play no part in the preemption analysis. *Mut. Pharm. Co. v. Bartlett*, 570 U.S. 472, 487-88 (2013) (holding that an "actor seeking to satisfy both his federal- and state-law obligations is not required to cease acting altogether in order to avoid liability"). "Indeed," the Court observed, "if the option of ceasing to act defeated a claim of impossibility, impossibility pre-emption would be all but meaningless." *Id.* at 488 (citation omitted).

85. [Moreover, disabling telematics would run headlong into new NHTSA reporting requirements. Pursuant to its statutory authority under 49 U.S.C. § 30166(g)(1)(A), NHTSA just issued a three-year standard reporting obligation to manufacturers of vehicles with certain telematics capabilities, to provide the agency with crash incident reports. See NHTSA, Standing General Order 2021-01 (June 29, 2021), [https://www.safercar.gov/sites/safercar.gov/files/2021-06/Standing\\_General\\_Order\\_2021\\_01-digital-06292021.pdf](https://www.safercar.gov/sites/safercar.gov/files/2021-06/Standing_General_Order_2021_01-digital-06292021.pdf). Disabling telematics would directly interfere with those reporting requirements.]

86. And it undisputed that it is a "practical impossibility" for manufacturers to disable telematics only for vehicles sold in the Commonwealth. Tierney Aff. ¶ 111; Garrie Aff. ¶ 86. [The Attorney General's proposal, then, would be to halt the nationwide progression of vehicle telematics technology dead in its tracks—and on a basis that even the voters of just one state, the Commonwealth, never intended. A law with "the practical effect [of] control[ling] conduct beyond the boundaries of the state" would be an unconstitutional extraterritorial mandate. *Healy v. Beer Inst. Inc.*, 491 U.S. 324, 336-37 (1989) (observing that the Commerce Clause prevents "the projection of one state regulatory regime into the jurisdiction of another State")]

87. [Indeed, the requirements of Data Access Law itself raise serious Commerce Clause concerns because its requirements cannot reasonably be cabined to Massachusetts—particularly the requirement to develop an entirely new platform for accessing vehicle data. The broad reach of that law into the data protection and access practices of national auto manufacturers would run afoul of the Commerce Clause. *See, e.g., Or. Waste Sys., Inc. v. Dep’t of Envtl. Quality*, 511 U.S. 93, 98 (1994) (“Though phrased as a grant of regulatory power to Congress, the [Commerce] Clause has long been understood to have a ‘negative’ aspect that denies the States the power unjustifiably to . . . burden the interstate flow of articles of commerce.”). It is well-established that, under the Commerce Clause, Massachusetts cannot “directly regulate[] . . . interstate commerce” *Brown-Forman Distillers Corp. v. N.Y. State Liquor Auth.*, 476 U.S. 573, 578 (1986); accord *Nat'l Foreign Trade Council v. Natsios*, 181 F.3d 38, 69 (1st Cir. 1999) (“Massachusetts may not regulate conduct wholly beyond its borders.”), *aff'd sub. nom., Crosby v. Nat'l Foreign Trade Council*, 530 U.S. 363 (2000).]

### C. Enforcement Provisions and Other Requirements

88. Section 4 of the Data Access Law directs the Attorney General “to establish for prospective vehicle owners a motor vehicle telematics system notice” that certain classes of dealerships would have to provide to prospective owners. Data Access Law§ 4 (codified at Mass. Gen. L. ch. 93K § 2(g)). The Attorney General has not yet issued the notice required under Section 4, and has informed the Court that she does not intend to do so until after the Court rules on the preemption claims now before the Court.

89. Section 5 of the Data Access Law imposes a broad range of penalties for violators. It permits vehicle owners and independent repair shops to sue auto manufacturers for violations of

the statute and recover treble damages or a minimum penalty of \$10,000 per event. Data Access Law § 5 (codified at Mass. Gen. L. ch. 93K § 6(e)).

90. It also grants the Attorney General of the Commonwealth broad enforcement authority, subjecting manufacturers to “any remedy authorized by chapter 93A” of the Massachusetts General Laws. Data Access Law § 5 (codified at Mass. Gen. L. ch. 93K § 6(e)). That means that if an auto manufacturer were to be unable to develop the data access systems required by the Data Access Law, the Commonwealth could seek injunctive relief against it, *see id.* ch. 93A, § 4, up to and including exclusion from the Massachusetts auto market entirely, *id.* § 8.

### **Conflict Preemption**

91. The U.S. Constitution’s Supremacy Clause “makes the laws of the United States ‘the supreme Law of the Land; any Thing in the Constitution or Laws of any State to the Contrary notwithstanding.’” *Hughes v. Talen Energy Mktg., LLC*, 136 S. Ct. 1288, 1297 (2016) (quoting U.S. Const. art. VI, cl. 2). In other words, “[p]ut simply, federal law preempts contrary state law.” *Id.*

92. The concept of preemption rests on the notion of federal supremacy in our federalist system. Despite solicitude for certain “state complementary action,” matters impacting interstate commerce are lodged decidedly in the federal domain. Thomas Reed Powell, *Vagaries & Varieties in Constitutional Interpretations* 176 (2002); *see also id.* at 164 (“[I]t is well to remember that in our constitutional federalism it is Congress and not the states which have power over interstate commerce because it is interstate commerce. Such powers as the states enjoy over such commerce derive *aliunde*, and the fact that interstate commerce is thereby regulated is a hurdle or a barrier

rather than a justification. The judgment as to the height of the barrier and as to the desirability of being permitted to surmount it is not a judgment that the state is free to make as it chooses.”).

93. Given the regulatory environment at issue here, the burden is on the Attorney General to point to a particular law that authorizes the Commonwealth to regulate the electronic architecture the country’s automotive industry uses to protective safety- and emissions-critical vehicle systems. See, e.g., Powell, *supra* at 163-64 (discussing the interplay between federal and state regulation). It is difficult to imagine a more national project. After all, as courts have observed in other contexts, “motor vehicles are the quintessential instrumentalities of interstate commerce.” *United States v. Bishop*, 66 F.3d 569, 588 (3d Cir. 1995) (internal quotations omitted); accord *United States v. McHenry*, 97 F.3d 125, 126 (6th Cir. 1996).

94. It is “beyond dispute that federal courts have jurisdiction over suits to enjoin state officials from interfering with federal rights.” *Shaw*, 463 U.S. at 96 n.14 (“A plaintiff who seeks injunctive relief from state regulation, on the ground that such regulation is pre-empted by a federal statute which, by virtue of the Supremacy Clause of the Constitution, must prevail, thus presents a federal question which the federal courts have jurisdiction under 28 U.S.C. § 1331 to resolve.”); accord *Verizon Md. Inc. v. Pub. Serv. Comm’n*, 535 U.S. 635, 642 (2002) (“We have no doubt that federal courts have jurisdiction under § 1331 to entertain [preemption suits].”); *Local Union No. 12004 United Steelworkers of Am. v. Massachusetts*, 377 F.3d 64, 74-75 (1st Cir. 2004) (discussing the continuing vitality of *Shaw*).

95. One species of preemption is conflict preemption. *Hughes*, 136 S. Ct. at 1297. Conflict preemption “occurs ‘when compliance with both state and federal law is impossible, or when the state law stands as an obstacle to the accomplishment of the full purposes and objectives of Congress.’” *Town of Acton v. W.R. Grace & Co.*, No. 13-12376-DPW, 2014 WL 7721850, at

\*9 (D. Mass Sept. 22, 2014) (quoting *Weaver's Cove Energy, LLC v. R.I. Coastal Res. Mgmt. Council*, 589 F.3d 458, 472 (1st Cir. 2009)).

96. The Court in *Geier* set forth the standard for analyzing conflict preemption. 529 U.S. at 870. It looks to whether, “under the circumstances of th[e] particular case,” the state law “stands as an obstacle to the accomplishment and execution of the full purposes and objectives of Congress—whether that ‘obstacle’ goes by the name of ‘conflict to; contrary to; . . . repugnance; difference; irreconcilability; inconsistency; violation; curtailment; . . . interference,’ or the like.” *Id.* at 873 (quoting *Hines v. Davidowitz*, 312 U.S. 52, 67 (1941)).

97. Conflict preemption analysis looks beyond express statutory language to the “purpose[s] and intended effects” of federal law. *Comm'n's Imp. Exp. S.A. v. Rep. of the Congo*, 757 F.3d 321, 326 (D.C. Cir. 2014) (internal citations omitted).

98. Thus, “federal law may preempt state law even if the conflict between the two is not facially apparent—as when, for example, the federal and state laws govern different subject matters.” *Comm'n's Imp.*, 757 F.3d at 326. The critical question is whether the state law serves “as an obstacle to the accomplishment and execution” of important “federal objectives,” *Geier*, 529 U.S. at 881, or renders it impossible to comply with both state and federal law, *see, e.g., Weaver's Cove*, 589 F.3d at 472 (internal citations omitted).

99. Plaintiff has demonstrated by a preponderance of the evidence two independent bases through which the Data Access Law is preempted by the Vehicle Safety Act.

#### **The Data Access Law Conflicts with the Purposes and Objectives of the Vehicle Safety Act**

100. The Data Access Law conflicts with the purposes and objectives of the Vehicle Safety Act.

101. Under the authority of the Motor Vehicle Safety Act, the Secretary of Transportation, acting through NHTSA, acts to safeguard the public through education, research, safety standards, and enforcement. 49 U.S.C. § 30101, *et seq.*

102. The Vehicle Safety Act confers twin authorities on NHTSA for the purpose of protecting the safety of motor vehicles. One is the authority to issue and enforce FMVSSs for new vehicles and equipment. 49 U.S.C. § 30111. FMVSSs issued pursuant to that section expressly preempt inconsistent state or local laws. *Id.* at 30103(b). But the statute also directs NHTSA to require manufacturers to issue notification and remedy campaigns—commonly called recalls—to address and remediate safety-related defects arising in vehicles. *Id.* §§ 30118-120. The Act requires manufacturers to initiate recalls when either NHTSA or the manufacturer identify a defect, *id.* §§ 30118(a), 30120(a), and also authorizes NHTSA to order a recall if the manufacturer does not commence one, *id.* § 30118(b)(2).

103. NHTSA achieves its agency objectives through its exercise of these twin authorities. As NHTSA recently noted, the “[Vehicle] Safety Act defines ‘motor vehicle safety’ as ‘the performance of a motor vehicle or motor vehicle equipment in a way that protects the public against unreasonable risk of accidents occurring because of the design, construction, or performance of a motor vehicle, and against unreasonable risk of death or injury in an accident, and includes nonoperational safety of a motor vehicle.’” 85 Fed. Reg. 83143, 83150 (Dec. 21, 2020) (quoting 49 U.S.C. 30102(a)(9)). That “common term”—vehicle safety—“is the driving force behind both FMVSS-setting and defect determinations, act[ing] to link NHTSA’s execution of its authorities against unreasonable safety risks inherently, both in setting FMVSS and in overseeing the safety of vehicle design, construction, and performance.” *Id.*

104. An important part of NHTSA’s oversight authority is ensuring that any safety-related defects are remedied, through vehicle recalls if necessary. 49 U.S.C. §§ 30118-120. Manufacturers also have a statutory obligation to monitor safety and notify NHTSA of any safety-related defects. *E.g., id.* § 30118(c). If NHTSA determines that a recall is required to remedy a condition under the Vehicle Safety Act, a state is preempted from requiring the manufacturer to create or maintain the vehicle condition giving rise to the recall because, under such circumstances, it would be impossible to comply with both the Vehicle Safety Act and the state law. See, e.g., id. § 30118(b) (lodging in the Secretary of the U.S. Department of Transportation—and through him or her, NHTSA—the authority to “decide” whether a “defect” is “related to motor vehicle,” and providing that the Secretary “shall order the manufacturer” to remedy any such defect).

105. Put simply, if NHTSA concludes that a particular condition is a “defect related to motor vehicle safety,” 49 U.S.C. 30118(b)(1), federal law requires the manufacturer to conduct a recall to fix the condition giving rise to that defect, *see id.* §§ 30119-120.

106. NHTSA buttresses its oversight authority by taking proactive steps to prevent the need for recalls in the first place. To that end, NHTSA occasionally publishes guidance for the automotive industry that it regulates on the agency’s interpretation of the term “defect related to motor vehicle safety,” 49 U.S.C. § 30118(b)(1), as that term applies in particular contexts or to particular conditions. A few years ago, for example, NHTSA issued guidance confirming that, if an aftermarket software update creates or introduces an unreasonable safety risk to motor vehicle systems, “then that safety risk constitutes a defect compelling a recall.” NHTSA, *Enforcement Guidance Bulletin*, 81 Fed. Reg. 65705, 65709 (Sept. 23, 2016).

107. Following on the heels of NHTSA’s September 2016 notice to the industry that it considers software problems as potentially constituting defects that would need to be remedied

under the Vehicle Safety Act, NHTSA released its October 2016 *Cybersecurity Best Practices for Modern Vehicles* to provide further guidance in this burgeoning area. See Ex. 3 at 5 (NHTSA, *Cybersecurity Best Practices for the Safety of Modern Vehicles* (2016) (discussing NHTSA's intent to encourage "proactively adopting and using available guidance such as this document and existing standards and best practices).

108. Guidance like this allows NHTSA to react nimbly to the evolution of cybersecurity threats and buttresses NHTSA's promulgation of formal safety standards, which recognize that vehicles increasingly depend on sophisticated technology to control essential functions. See, e.g., 49 C.F.R. § 571.126 (mandating minimum safety standards for electronic stability control systems in lightweight passenger vehicles, which controls among other things vehicle steering, braking, and speed by computer means).

109. Although agency guidance does not itself have preemptive effect, the Supreme Court has recognized that an agency's views are highly probative in determining preemption because the agency "is likely to have a thorough understanding of its own regulation and its objectives and is uniquely qualified to comprehend the likely impact of state requirements." *Geier*, 529 U.S. at 883. And agency guidance provides insight into what an agency views its purposes and objectives to be. See, e.g., *Altra Grp., Inc. v. Good*, 555 U.S. 70, 89 (2008) (considering FTC policy guidance but after reviewing it concluding that "the FTC has no longstanding policy authorizing collateral representations").

110. NHTSA has enforced its view that manufacturers must install and maintain appropriate cybersecurity controls to avoid the exercise of NHTSA's recall authority under 49 U.S.C. §§ 30118-120. In 2015, NHTSA found that some Chrysler vehicles had a flaw in their radio software security that could allow unauthorized third-party access to some networked vehicle

control systems. Specifically, NHTSA determined that third-party exploitation of the software security vulnerabilities could lead to exposing the driver, the vehicle occupants or any other individual or vehicle with proximity to the affected vehicle to a potential risk of injury. Ultimately, Chrysler worked with NHTSA to issue a voluntary recall of 1,410,000 vehicles to repair the software vulnerability and avoid a finding of a statutory violation. *See Findings of Fact ¶¶ 83-87.*

111. *And NHTSA has observed that the Data Access Law implicates these motor vehicle safety concerns. Although manufacturers retain some flexibility in precisely how to safeguard safety-critical vehicle systems, the agency has made clear that those systems must be protected in ways that are antithetical to the requirements of the Data Access Law—e.g., through manufacturers controlling access to firmware that executes core vehicle functions like acceleration, braking, and steering; isolating vehicle systems from one another; and maintaining non-standardized approaches across the industry to prevent large-scale hacking. See Findings of Fact ¶¶ 64-79, 108-29.*

112. *NHTSA has thus made clear both that (a) failure to maintain adequate cybersecurity controls would give rise to a safety-related defect, and hence recall obligations under the Vehicle Safety Act; and (b) the Data Access Law's requirements cannot be satisfied by manufacturers without removing current cybersecurity controls that are critical for maintaining vehicle safety. Findings of Fact ¶¶ 64-79, 108-29.*

113. *The United States indicated, in this case, that depending on how manufacturers attempt to comply with the Data Access Law, a recall could be required. U.S. Statement of Interest (Dkt. 202) at 9. As experts for both parties agreed, the gateway in modern vehicles would have to be substantially altered, if not disabled entirely. Findings of Fact ¶ 144-46; Bort Aff. ¶¶ 56, 86-87, 101-02. But doing so would only put manufacturers, including FCA, in the same position they*

found themselves in in 2014—when hackers infiltrated FCA vehicles and ultimately caused a recall. Findings of Fact ¶ 83-87; see also U.S. Statement of Interest (Dkt. 202) at 5-9.

114. Based on the evidence introduced at trial, the Data Access Law would require manufacturers to take steps counter to the purposes and objectives of the Vehicle Safety Act. Findings of Fact ¶¶ 64-79. Because compliance with the Data Access Law would present an obstacle to the purposes and objectives of the Vehicle Safety Act and the Data Access Law, there is a clear conflict between federal and state law and the state law must yield. U.S. Const. art. VI. Accordingly, the Data Access Law is preempted by the Vehicle Safety Act and thus void and unenforceable.

#### **The Data Access Law Directly Conflicts with the Vehicle Safety Act**

115. The Data Access Law directly conflicts with, and is consequently preempted by, Section 30122(b) of the Vehicle Safety Act. 49 U.S.C. § 30122(b).

116. The Data Access Law requires automobile manufacturers to remove cybersecurity controls and degrade cybersecurity protection. Findings of Fact ¶¶ 64-79, 108-29.

117. The Vehicle Safety Act prohibits auto manufacturers from removing or otherwise degrading critical safety features like cybersecurity controls. 49 U.S.C. § 30122(b). A “manufacturer . . . may not knowingly make inoperative any part of a device or element of design installed on or in a motor vehicle or motor vehicle equipment in compliance with an applicable motor vehicle safety standard prescribed under this chapter.” *Id.*

118. Section 30122(b) of the Vehicle Safety Act applies not only to features specifically identified as required in a motor vehicle safety standard. By its plain terms, the statute applies to “any . . . element of design” that the manufacturer “installed on or in a motor vehicle” to comply with a safety standard. 49 U.S.C. § 30122(b) (emphasis added).

119. Manufacturers have installed a variety of cybersecurity protections around regulated vehicle functions to help prevent threat actors (or others) from taking control of core vehicle functions and, ultimately, the vehicle itself. Findings of Fact ¶¶ 23-61, 65-66, 67-68, 70-71, 73-74, 76-77. These cybersecurity protections are key “part[s]” of the “device or element of design” of vehicles, which allow them to comply with federal motor vehicle standards. 49 U.S.C. § 30122(b).

120. Specifically, manufacturers’ cybersecurity design elements protect core vehicle functions like acceleration, braking, steering, and air bags. Several “motor vehicle safety standard[s]” are “applicable.” 49 U.S.C. § 30122(b). NHTSA regulates extensively in the areas of acceleration, braking, steering, and air bags. *See* 49 C.F.R. § 571.124 (acceleration control devices); *id.* § 571.126 (electronic stability control—including steering and anti-lock braking systems (“ABS”)); *id.* § 571.135 (light-vehicle braking systems); *id.* § 571.208 (occupant crash protection—including air bags).

121. FMVSS 124 regulates acceleration control systems. *See* 49 C.F.R. § 571.124. The standard encompasses nearly anything related to how the accelerator functions—“all vehicle components, except the fuel metering device, that regulate engine speed in direct response to movement of the driver-operated control and that return the throttle to the idle position upon release of the actuating force.” *Id.* And the standard presupposes that *the driver*—not some threat actor—will be in control of a vehicle’s acceleration. It describes the feature it covers as a “[d]river-operated accelerator control system” and “establishes requirements for the return of a vehicle’s throttle to the idle position when *the driver* removes the actuating force from the accelerator control.” *Id.* (emphasis added). Manufacturers have installed cybersecurity

protections over accelerator functions that are key “parts” of the “device or element of design” of vehicles, which allow them to comply with federal motor vehicle standards. 49 U.S.C. § 30122(b).

122. The FMVSS for light vehicle brake systems has the broad purpose of insuring “safe braking performance under normal and emergency conditions.” 49 C.F.R. § 571.135 (FMVSS 135). As with acceleration control devices, this FMVSS necessarily presupposes that *the driver*—not some threat actor—remains in control of braking. *See, e.g., id.* (stating that any brake power assist unit must ensure that while “reduc[ing] the amount of muscular force that *a driver* must apply to actuate the system” it “does not prevent *the driver* from braking the vehicle by a continued application of muscular force”); *id.* (discussing a brake power unit as involving the “*driver* action . . . of modulating the energy application level”); *id.* (discussing brake testing conditions to include “[p]edal force . . . applied and controlled by *the vehicle driver*) (emphases added). Manufacturers have installed cybersecurity protections over braking functions that are key “parts” of the “device or element of design” of vehicles, which allow them to comply with federal motor vehicle standards. 49 U.S.C. § 30122(b).

123. Much the same is true for steering and ABS. Vehicle electronic stability control (“ESC”) systems are “computer-controlled with the computer using a closed-loop algorithm to limit vehicle oversteer and to limit vehicle understeer.” 49 C.F.R. § 571.126 (FMVSS 126). The safe and approved operation of these systems relies on manufacturers to ensure that electronic inputs come from the driver, and that the driver remain in control. *See, e.g., id.* (describing the approved system as a “means to monitor *driver* steering inputs”); *id.* (requiring the “algorithm to determine the need, and a means to modify engine torque, as necessary, to assist *the driver* in maintaining control of the vehicle”); *id.* (discussing *the driver’s* ability “disable[] [the] ESC” system) (emphases added). Manufacturers have installed cybersecurity protections over steering

and ABS functions that are key “parts” of the “device or element of design” of vehicles, which allow them to comply with federal motor vehicle standards. 49 U.S.C. § 30122(b).

124. The FMVSS for occupant crash protection contemplates that the air bags will deploy only in the event of a triggering collision. 49 C.F.R. § 571.208 (air bags) (contemplating that the “vehicle is in a crash severe enough to cause the air bag to inflate”). Manufacturers have installed cybersecurity protections over air bag functions that are key “parts” of the “device or element of design” of vehicles, which allow them to comply with federal motor vehicle standards. 49 U.S.C. § 30122(b).

125. Based on the evidence adduced at trial, the Data Access Law would require manufacturers to make inoperative cybersecurity design elements that they installed on vehicles to meet the requirements of FMVSSs 124, 126, 135, and 208. Findings of Fact ¶ 23-61, 65-66, 67-68, 70-71, 73-74, 76-77; see also id. ¶¶ 113-57 (discussing how no technology presently exists that would allow manufacturers to comply with both the Vehicle Safety Act and the Data Access Law). Because manufacturers cannot comply with both the Vehicle Safety Act and the Data Access Law, there is a clear conflict between federal and state law and the state law must yield. U.S. Const. art. VI. Accordingly, the Data Access Law is preempted by the Vehicle Safety Act and thus void and unenforceable.

#### **The Data Access Law is Preempted by the Clean Air Act**

126. Through the Clean Air Act, Congress has established a comprehensive statutory scheme to control air pollution from all sources throughout the nation. 42 U.S.C. §§ 7401, *et seq.*

127. The Clean Air Act carefully delineates responsibilities between the federal government and the states. Title I of the Act, 42 U.S.C. §§ 7401-7515, vests the states, under EPA’s supervision, with the authority to regulate stationary sources (*e.g.*, factories and power plants) located within their borders. *Motor Vehicle Mfrs. Ass’n v. N.Y. Dep’t of Envtl.*

*Conservation*, 17 F.3d 521, 525 (2d Cir. 1994). With certain limited exceptions not applicable here, Title II of the Act, 42 U.S.C. §§ 7521-90, vests the federal government, acting through EPA, with exclusive authority to regulate mobile sources (e.g., cars, trucks, buses, aircraft, locomotives, farm and construction equipment, and ships). *Id.* §§ 7521, 7547, and 7543.

128. For reasons similar to the Vehicle Safety Act, Plaintiff has demonstrated by a preponderance of the evidence that the Data Access Law is preempted by the Clean Air Act. The Data Access Law “stands as an obstacle to the accomplishment and execution of the full purposes and objectives of Congress” in the Clean Air Act. *Oneok, Inc. v. Learjet, Inc.*, 575 U.S. 373, 377 (2015) (internal quotations and citations omitted).

129. The Clean Air Act imposes stringent vehicle emissions requirements on manufacturers including warranting the emission control system of vehicles they manufacture for the “useful life” of the vehicle—either 10 years or 100,000 miles. 42 U.S.C. § 7521(d), 7541(a)(1). As part of this obligation, manufacturers must, for example, perform in-use verification testing on post-sale vehicles at regular mileage intervals prescribed by federal regulation. 42 C.F.R. § 86.1845-04.

130. Under the Clean Air Act, it is a violation of federal law for “any person to remove or render inoperative any device or element of design installed on or in a motor vehicle engine in compliance with regulations under [the Act] prior to its sale and delivery to the ultimate purchaser, or for any person knowingly to remove or render inoperative any such device or element of design after such sale and delivery to the ultimate purchaser.” 42 U.S.C. § 7522(a)(3)(A).

131. The language of the Clean Air Act broadly encompasses “any . . . element of design.” See 42 U.S.C. § 7522(a)(3)(A) (emphasis added). The element of design need not itself be explicitly required by applicable regulations. *Id.*

132. Federal EPA regulations confirm the broad nature of design elements, as used in the Clean Air Act. They provide that an “element of design” includes “any control system (i.e., computer, software, electronic control system, emission control system, computer logic)” in the vehicle. 40 C.F.R. § 86.1803-01.

133. Manufacturers have installed cybersecurity protections around the engine control module that could be considered “element[s] of design.” 42 U.S.C. § 7522(a)(3)(A).

134. If manufacturers are required to remove cybersecurity protections on existing vehicles, those modifications would have to be assessed for emissions impact. At the very least, the Data Access Law’s requirements (and timeline to meet those requirements) mean that manufacturers would have to eliminate or thoroughly degrade existing cybersecurity controls that help to protect against cyber intrusion of emissions-related vehicle components. Findings of Fact ¶¶ 5, 24, 88-96.

135. The evidence adduced at trial demonstrates that these required changes to cybersecurity protections would more readily allow vehicle owners or third parties access to a vehicle’s engine control module to disable emissions control systems via aftermarket software designed for that purpose. Findings of Fact ¶¶ 92-96.

136. Based on the evidence adduced at trial, the Data Access Law would require manufacturers to remove cybersecurity design elements. Because manufacturers cannot comply with both the Clean Air Act and the Data Access Law, there is a clear conflict between federal and state law and the state law must yield. U.S. Const. art. VI. Accordingly, the Data Access Law is preempted by the Clean Air Act and thus void and unenforceable.

### **Severability**

137. The Data Access Law's provisions are not severable. As one cohesive ballot initiative, the Data Access Law necessarily addresses “subjects which are related or which are mutually dependent.” Mass. Const. amends. art. LXXIV.

138. Because of this requirement, even a ballot initiative that contains a severability clause would raise a “challenging” issue as to its effect. *Mass. Teachers Ass'n v. Sec'y of Com.*, 384 Mass. 209, 233 (1981) (“The concept that subjects which have to be ‘related’ may nevertheless be severable is a challenging one.”). The Supreme Judicial Court declined to decide the severability issue in that case only because it found the entire statute constitutional. *Id.*; *see also Anderson v. Attorney General*, 479 Mass. 780, 785 (2018) (“The mandate that an initiative petition contain a single ‘common purpose’ arises because a voter, unlike a legislator, ‘has no opportunity to modify, amend, or negotiate the sections of a law proposed by popular initiative.’ A voter cannot ‘sever the unobjectionable from the objectionable,’ and must vote to approve or reject an initiative petition in its entirety.”) (internal citations omitted); *Abdow v. Attorney General*, 468 Mass. 478, 509 (2014) (reserving judgment on the “legal effect of the severability language” itself in a ballot initiative).

139. The ballot initiative that gave rise to the Data Access Law does not contain a severability clause. *See generally* Data Access Law.

140. The same principles apply to the Attorney General's newfound argument that the Court should strike and “sever” the Data Access Law's effective date in Section 3. *Attorney General's Post-Evidence Mem* 17-18 (Dkt. 217).

141. Courts do not engage in “quintessentially legislative” activity to save a statute that has been deemed at least partially unconstitutional. *Ramirez v. Commonwealth*, 479 Mass. 331, 338 (2018) (internal quotations omitted). It is one thing to “excis[e] an invalid provision from an

otherwise valid [statute].” *Greater Boston Real Estate Bd. v. City of Boston*, 428 Mass. 797, 804 (1999). It is quite another to excise that provision, weigh technological capabilities and cybersecurity risks, and set a new effective date. That is exactly what severing the effective date in the way the Attorney General requests would require.

142. Striking the effective date of Model Year 2022 would leave the statute’s effective date to be defined by background principles of Massachusetts law. Under those principles, ballot initiatives take effect thirty days after the election. See Mass. Const. Amends. Art. 48, Pt. V, § 1. That would make the Data Access Law effective as of December 3, 2020. What the Attorney General requests is judicial legislation to determine a new effective date that would allow manufacturers sufficient time to *safely comply* with the Data Access Law and their obligations under federal law. The Model Year 2022 requirement cannot be severed in this way.

143. Staying the effective date pending resolution on appeal presents a separate set of issues but is equally inadequate. Without a declaration that the Data Access Law is invalid, a stay could only bind the Attorney General. But the Data Access Law contains a private right of action, allowing independent repair shops and vehicle owners to sue manufacturers. Data Access Law § 5 (codified at Mass. Gen. L. ch. 93K § 6(e)). Therefore, the most appropriate resolution in this case is to strike down the Data Access Law in full.

### **Relief**

144. The Plaintiff properly seeks declaratory and injunctive relief. See, e.g., *Algonquin Gas Transmission, LLC v. Weymouth, Mass.*, 919 F.3d 54, 65-66 (1st Cir. 2019) (affirming declaratory judgment finding state statute preempted by federal law); *SPGGC, LLC v. Ayotte*, 488 F.3d 525, 536 (1st Cir. 2007) (affirming declaratory judgment holding state law preempted by federal law); *De Jesus v. Am. Airlines, Inc.*, 532 F. Supp. 2d 345, 355 (D. Puerto Rico 2007)

(granting declaratory relief and permanent injunction in preemption case); *United Parcel Serv., Inc. v. Flores-Galarza*, 210 F. Supp. 2d 33, 44 (D. Puerto Rico 2002) (granting permanent injunction based on preemption of territorial law by federal law).

145. The Plaintiff has shown that its manufacturer members (1) will suffer “irreparable injury; (2) that remedies available at law, such as monetary damages, are inadequate to compensate for that injury; (3) that, considering the balance of hardships between the parties, a remedy in equity is warranted; and (4) that the public interest would not be disserved by a permanent injunction.” *Global NAPs, Inc. v. Verizon New England, Inc.*, 706 F.3d 8, 13 (1st Cir. 2013) (quoting *eBay Inc. v. MercExchange, L.L.C.*, 547 U.S. 388, 391 (2006)) (brackets omitted).  
Accordingly:

146. The Court rules that the Data Access Law is unenforceable because it is preempted by the Vehicle Safety Act.

147. The Courts rules that the Data Access Law is unenforceable because it is preempted by the Clean Air Act.

148. Enforcement of the Data Access Law is permanently enjoined.

Dated: July 14, 2021

Respectfully submitted,

ALLIANCE FOR AUTOMOTIVE INNOVATION

By its attorneys,

/s/ Laurence A. Schoen

John Nadolenco (*pro hac vice*)  
Erika Z. Jones (*pro hac vice*)  
Jason D. Linder (*pro hac vice*)  
Daniel D. Queen (*pro hac vice*)  
Eric A. White (*pro hac vice*)  
MAYER BROWN LLP

1999 K Street, NW  
Washington, DC 20006  
Tel: (202) 263-3000  
jnadolenco@mayerbrown.com  
ejones@mayerbrown.com  
jlinder@mayerbrown.com  
dqueen@mayerbrown.com  
eawhite@mayerbrown.com

Laurence A. Schoen, BBO # 633002  
Elissa Flynn-Poppey, BBO# 647189  
Andrew N. Nathanson, BBO#548684  
MINTZ, LEVIN, COHN, FERRIS,  
GLOVSKY, AND POPEO, P.C.  
One Financial Center  
Boston, MA 02111  
Tel: (617) 542-6000  
lschoen@mintz.com  
eflynn-poppey@mintz.com  
annathanson@mintz.com

Charles H. Haake (*pro hac vice*)  
Jessica L. Simmons (*pro hac vice*)  
ALLIANCE FOR AUTOMOTIVE INNOVATION  
1050 K Street, NW  
Suite 650  
Washington, DC 20001  
Tel: (202) 326-5500  
chaake@autosinnovate.org  
jsimmons@autosinnovate.org

**CERTIFICATE OF SERVICE**

The foregoing document was served on counsel for the defendant by electronic mail.

/s/ Laurence A. Schoen